Jaarverslag Informatiebeveiliging 2019

Gemeente Landsmeer



Definitieve versie 1.0

Gemeente Landsmeer

Inhoudsopgave

	Hoofdstuk/Paragraaf	Pagina
Inhoudsopgave		
Bijlagen		
	1. Inleiding	4
	2. Visie, doelstellingen en ambities	6
	3. Activiteiten en verbetermaatregelen 2019	7
	3.1 Organisatie en sturing	7
	3.2 Beleid	7
	Beleid Informatiebeveiliging	7
	Beleid Privacy	7
	3.3 Nulmeting	8
	Nulmeting Informatiebeveiliging	8
	Nulmeting Privacy	8
	3.4 Implementatieplan 'Privacy in Control'	8
	3.5 Bewustwording	8
	Test phishing-mail	9
	Mystery Guest	9
	Awareness sessie gemeentebreed	9
	Informatie intranetsite	9
	10-gouden regels	10
	Bewustwording teammanagers	10
	3.6 Verwerkersovereenkomsten	10
	3.7 Beveiligingsniveau processen	11
	3.8 ENSIA audit	11
	Resultaat ENSIA audit	12
	Van BIG naar BIO	14
	3.9 Beveiligingsincidenten 2019	15
	3.10 Datalekken 2019	15
	3.11 Privacyverklaring	15
	3.12 Data Protection Impact Assessment	15
	3.13 Conclusie	16
	4. Doorkijk naar 2020	17
	4.1 Gebeurtenissen met grote impact op de informatieveiligheid en privacy	17
	Beveiligingslek Citrix	17
	Coronacrisis	17
	4.2 Projecten in 2020	18
	i-Navigator	18
	Verwerkingsregister	18
	Basisbeveiligingsniveau (BBN)	18
	Information Security Management System (ISMS)	19
	SIEM SOC	19
	4.3 Overige activiteiten en werkzaamheden in 2020	19
	Informatiebeveiliging en privacy binnen het inkoopproces	19
	Diverse protocollen en procedures	20
	Nulmeting Informatiebeveiliging	20

	Nulmeting Privacy	20
	ENSIA audit	20
	Bewustwording	20

Bijlage	
Bijlage 1:	Collegeverklaring 2019
Bijlage 2:	Assurance Rapportage 2019
Bijlage 3:	Verantwoordingsrapportage BAG 2019
Bijlage 4:	Verantwoordingsrapportage BGT 2019
Bijlage 5:	Verantwoordingsrapportage BRO 2019
Bijlage 6:	Verantwoordingsrapportage Reisdocumenten 2019
Bijlage 7:	Verantwoordingsrapportage BRP 2019

Versie	Steller	Besproken met	Opmerkingen	Datum
Concept 0.1	Carina Kampstra CISO/PO	- Dhr. D. Straat / Burgemeester - Mevr. S. van Geffen / Secretaris - Dhr. B. Bilyj / Teammanager Ondersteuning - Dhr. R. Rekoert / Functionaris Gegevensbescherming	- Verschil benoemen tussen het jaarverslag Informatiebeveiliging en de jaarrapportage Privacybescherming; - Duidelijke omschrijving van de verschillende manieren van verantwoording.	29 juni 2020
Concept 0.2		Strategisch overleg IB/P		31 augustus 2020
Definitief 1.0			**Geen verdere opmerkingen**	

1 Inleiding

Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor de uitvoering van de taken en verantwoordelijkheden van de gemeente Landsmeer. Omdat de gemeente onderdeel uitmaakt van de totale overheid en ook verbonden is met andere ketenpartijen, kan een onveilige situatie bij de gemeente Landsmeer ook direct gevolgen hebben voor de betrouwbaarheid van de dienstverlening door andere overheden of organisaties. Een goede informatiebeveiliging bij de gemeente is dus belangrijk voor het verlenen van een betrouwbare dienstverlening aan de inwoners van Landsmeer, maar ook voor het imago van de overheid in bredere zin.

Verantwoording aan de raad
In de resolutie '*Informatieveiligheid, randvoorwaarde voor de professionele gemeente*' is afgesproken om de raad te informeren over informatieveiligheid zodat zij haar toezichthoudende rol kan vervullen. In de programmabegroting binnen de paragraaf Bedrijfsvoering wordt verantwoording afgelegd over informatieveiligheid. Veel gemeenten kiezen daarnaast echter voor een separate rapportage aan de raad omdat een dergelijke rapportage bredere informatie biedt.

Jaarverslag Informatiebeveiliging 2019
Ook het college van de gemeente Landsmeer biedt de raad een separaat jaarverslag Informatiebeveiliging aan. In dit verslag wordt de stand van zaken betreffende informatiebeveiliging over het jaar 2019 beschreven en worden uitgevoerde relevante activiteiten en verbetermaatregelen toegelicht. Ook beschrijft het de uitkomsten van de ENSIA verantwoording. ENSIA staat voor Eenduidige Normatiek Single Information Audit. Middels dit jaarverslag wordt door het college dan ook verantwoording over informatiebeveiliging aan de raad afgelegd.

Jaarrapportage Gegevensbescherming 2019
Daarnaast biedt de Functionaris Gegevensbescherming (FG) afzonderlijk van dit jaarverslag Informatiebeveiliging een jaarrapportage Gegevensbescherming aan zowel het college als de raad aan, waarin de FG verslag doet over de stand van zaken ten aanzien van privacy compliance bij de gemeente Landsmeer.

Informatiebeveiliging en privacy compliance kan niet volledig los van elkaar gezien worden: voor het borgen van de bescherming van persoonsgegevens zijn passende beveiligingsmaatregelen van cruciaal belang. Onderwerpen welke in dit jaarverslag Informatiebeveiliging besproken worden zullen dan ook enige overlap met de jaarrapportage Gegevensbescherming kennen.

ENSIA audit
In 2019 hebben alle gemeenten voor de derde keer middels de ENSIA systematiek de stand van zaken wat betreft informatiebeveiliging in kaart gebracht. ENSIA nam in 2019 de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt. De scope van de ENSIA verantwoording betreft de:
- Implementatie Baseline Informatiebeveiliging Gemeenten (BIG)
- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling Nederland (PUN)
- Digitale persoonsidentificatie (DigiD)

- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Gezamenlijke Elektronische Voorziening Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Een verkorte weergave van de uitkomsten van de ENSIA verantwoording treft u aan in dit jaarverslag.

Tenslotte geeft dit jaarverslag over 2019 ook een doorkijk naar de geplande activiteiten en werkzaamheden voor 2020.

2 Visie, doelstellingen en ambities

Informatie is één van de voornaamste bedrijfsmiddelen van gemeente Landsmeer. Het verlies van (persoons)gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie en/of persoonsgegevens kan ernstige gevolgen hebben voor de bedrijfsvoering maar kan daarnaast ook leiden tot imagoschade.
Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke gevolgen. Informatieveiligheid en privacy is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

Visie
De komende jaren zet de gemeente Landsmeer in op het implementeren en borgen van noodzakelijke maatregelen met betrekking tot privacy, informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie.
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven.

Doelstelling
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Doelstelling is het waarborgen van de continuïteit van de informatiesystemen en minimaliseren van gevolgen voortkomend uit incidenten. En binnen de wettelijke kaders ervoor zorgen dat gemeentelijke informatie adequaat wordt beheerd en beveiligd.

3 Activiteiten en verbetermaatregelen 2019

Zowel de toenmalige Chief Information Security Officer (CISO) als ook de Privacy Officer (PO) hebben eind 2018/begin 2019 de organisatie verlaten. Hierdoor is de doorontwikkeling van informatieveiligheid en de implementatie AVG vanaf dat moment stil komen te liggen.

Door deze ontwikkelingen waren er voor het jaar 2019 geen doelen bepaald voor de verdere implementatie van informatieveiligheid en de AVG.

Ondanks bovenstaande zijn er vooral in de tweede helft van 2019 werkzaamheden uitgevoerd. Hieronder volgt een korte beschrijving aan welke activiteiten binnen de organisatie uitvoering is gegeven en wat het behaalde resultaat is.

3.1 Organisatie en sturing

In juli 2019 heeft de beveiligingsorganisatie opnieuw vorm gekregen. Er is een Chief Information Security Officer (CISO) en Privacy Officer (PO) per 1 juli 2019 aangesteld, beide rollen zijn in één functie belegd, t.w. de CISO/PO. Dit is een fulltime functie. Door deze aanstelling zijn vanaf 1 juli 2019 weer werkzaamheden verricht op het gebied van informatieveiligheid en privacy.

Vanaf augustus 2019 vindt er periodiek (elke 2 maanden) een strategisch overleg Informatiebeveiliging/Privacy plaats. Hierbij zijn de burgemeester, secretaris, Functionaris Gegevensbescherming (FG) en CISO/PO vertegenwoordigd. Afhankelijk van het onderwerp welke besproken wordt binnen het overleg, neemt ook de Teammanager Ondersteuning deel aan het overleg. Indien nodig vindt tussentijds overleg/afstemming plaats. De gemeenteraad wordt onder andere via de jaarlijkse ENSIA verantwoording en het jaarverslag geïnformeerd over ontwikkelingen op het gebied van informatiebeveiliging en privacy.

3.2 Beleid

Beleid stelt kaders en richtlijnen inzake het beschermen van bedrijfsinformatie en (persoons)gegevens. Daarnaast wordt met beleid de verantwoordelijkheden belegd.

Beleid Informatiebeveiliging

Het informatiebeveiligingsbeleid was in 2014 door het college vastgesteld voor een periode van 4 jaar. Op 3 december 2019 is het '*Strategisch Informatiebeveiligingsbeleid 2019-2022*' door het college vastgesteld en vervangt hiermee het '*Informatiebeveiligingsbeleid 2014-2018'*.

Beleid Privacy

Er is een privacy beleidskader opgesteld en deze is op 23 juli 2019 door het college vastgesteld. Dit '*Privacy Beleidskader 2019'* wordt elke 2 jaar geëvalueerd en geactualiseerd.

3.3 Nulmeting

Om inzichtelijk te krijgen wat de stand van zaken is wat betreft de informatieveiligheid en de implementatie van de AVG, kan een nulmeting uitgevoerd worden. Hierbij wordt in kaart gebracht wat de organisatie al heeft geïmplementeerd en wat nog gedaan moet worden.

Nulmeting informatieveiligheid

Voor de informatieveiligheid kan de '*GAP-analyse BIO'* van de VNG/IBD ingezet worden. Voor 2019 is er geen nulmeting verricht. Voor het jaar 2020 wordt een nulmeting verricht met ondersteuning van een externe partij (Sincerus).

Nulmeting implementatie AVG

De FG en de CISO/PO hebben in juli 2019 een nulmeting AVG uitgevoerd. Er is gebruik gemaakt van het product '*Criteria borging AVG / Bijlage borgingsproduct gegevensbescherming in de gemeentelijke organisatie*' van de IBD/VNG. De nulmeting bestond uit zeven onderwerpen, namelijk:



- ✓ Beleid;
- ✓ Processen;
- ✓ Organisatorische inbedding;
- ✓ Rechten van betrokkenen;
- ✓ Samenwerking;
- ✓ Beveiliging;
- ✓ Verantwoording.

Van de 188 vragen is 34 met 'ja' (groen), 80 met 'nee' (rood), 17 met 'onbekend' (geel), 8 met 'niet van toepassing' (grijs) en 49 met 'gedeeltelijk' (oranje) beantwoord. Doordat door het vertrek van de CISO en PO de implementatie lang heeft stilgelegen (ruim een half jaar), is de score erg laag. Groen is waar de gemeente Landsmeer aan voldoet en rood geeft aan waar nog niet aan voldaan wordt.

3.4 Implementatieplan 'Privacy in Control'

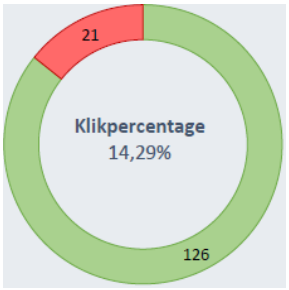
Naar aanleiding van de score uit de nulmeting is een implementatieplan opgesteld inclusief een planning. Alle in de planning genoemde onderwerpen zijn nodig om 'AVG compliant' te worden. Om goed inzicht in de planning te hebben en te houden, wordt in kleur de stand van zaken aangegeven.

3.5 Bewustwording

Er is in 2019 op verschillende manieren aandacht besteed aan het vergroten van de bewustwording van medewerkers voor het onderwerp Informatiebeveiliging en Privacy. Veelal wordt gedacht dat informatiebeveiliging een 'ICT-dingetje' is, terwijl juist de medewerker een grote bijdrage kan en moet leveren op het gebied van informatieveiligheid en privacy. Onderzoeken tonen namelijk aan dat de meeste beveiligingsincidenten nog steeds veroorzaakt worden door menselijk handelen. Op verschillende manieren wordt dan ook uitgebreid aandacht besteed aan het vergroten van de bewustwording van de medewerkers.

Test-phishingmail

In december 2019 is in samenwerking met een externe partij (NextTech Security) een test-phishingmail binnen de organisatie uitgezet. Enerzijds om bewustwording te creëren, anderzijds om de mate van bewustzijn bij de medewerkers te kunnen meten. Wanneer een medewerker op de link klikte die bij de test-phishingmail was toegevoegd, kwam de medewerker op een landingspagina terecht waar uitgelegd werd wat een phishingmail is en hoe deze herkend kan worden. Het klikpercentage was ruim 14%. Dit ligt onder het gemiddelde van de metingen van Next Tech Security (21%) bij andere organisaties, maar met deze uitkomst lopen we als organisatie nog steeds een hoog risico bij een echte phishingmail aanval.



Mystery guest

Ook is er in december 2019 een mystery guest (hierna: MG) onderzoek uitgevoerd. Voor het bezoek heeft de MG zich vermomd als printermonteur van het merk Canon. Bij het bezoek is het excuus gebruikt dat de onderzoeker uit naam van Canon een software-update kwam uitvoeren voor een betere beveiliging.
Tijdens het onderzoek heeft de MG geprobeerd zoveel mogelijk inzicht te krijgen in kwetsbaarheden zoals:

- ✓ Ongeautoriseerd toegang tot het pand en werkruimtes;
- ✓ Niet-vergrendelde werkstations;
- ✓ Opgeschreven wachtwoorden;
- ✓ Het kunnen achterhalen van inloggegevens en andere vertrouwelijke gegevens;
- ✓ Toegang tot informatie en dossiers in kasten en bij printers;
- ✓ Kwetsbaarheden van medewerkers met betrekking tot social engineering.

Uit het onderzoek is gebleken dat er binnen de gemeente Landsmeer de nodige ruimte is voor verbetering op bovengenoemde kwetsbaarheden.

Awareness-sessie organisatiebreed

In januari 2020 zijn de resultaten van de test phishing-mail en het MG onderzoek in een awareness sessie met de medewerkers besproken. Hier werden ook enkele filmpjes getoond van collega's die met de verborgen camera door de mystery guest waren gefilmd en de mystery guest toegang gaven tot hun werkplek. Met de betrokken medewerkers is besproken of ze akkoord gingen met het tonen van de filmpjes. Deze beelden hebben tijdens de awareness sessie veel indruk gemaakt op de collega's. Daarnaast werden in deze sessie ook veel tips gegeven over hoe je een phishing mail kunt herkennen, waar een veilig wachtwoord aan moet voldoen, hoe je je wachtwoorden kunt opslaan in een 'wachtwoordenkluis' e.d.

Informatie intranet

Veel informatie over informatieveiligheid en privacy wordt via intranet aangeboden in de vorm van korte, duidelijke berichten. Daarnaast is ook een intranetpagina Informatiebeveiliging/privacy beschikbaar waar allerlei relevante documenten over dit onderwerp te vinden zijn.

10 gouden regels
Op elke deur van de werkkamers is een poster met de 10 gouden regels opgehangen. Dit als een geheugensteun hoe de medewerker zelf op éénvoudige wijze kan (en moet) bijdragen aan het op een veilige manier omgaan met (gevoelige) informatie en persoonsgegevens.

Bewustwording management
Bij bewustwording specifiek gericht op de teammanagers is vooral aandacht besteed aan de verantwoordelijkheden die zij hebben wat betreft de informatiebeveiliging en privacy binnen hun processen. Aandacht voor bewustwording heeft plaatsgevonden door middel van presentaties. De volgende presentaties hebben plaatsgevonden:

- ✓ '*Stand van zaken Informatiebeveiliging en Privacy*'. Hier was vooral aandacht voor de ENSIA audit over het verantwoordingsjaar 2019;
- ✓ '*Verwerkersovereenkomsten*'. In deze presentatie werd ingegaan op wat een verwerkersovereenkomst is en wanneer en waarom een verwerkersovereenkomst nodig is;
- ✓ '*Informatiebeveiliging en privacy en de rol van de teammanagers*'. In deze presentatie stond vooral de opzet van de BIO centraal en welke rol en verantwoordelijkheden de teammanagers hierbij hebben.



3.6 verwerkersovereenkomsten

In vervolg op de presentatie over verwerkersovereenkomsten is een begin gemaakt met het inventariseren van de verwerkersovereenkomsten binnen de gemeente Landsmeer. Wanneer de gemeente Landsmeer werkzaamheden waarbij persoonsgegevens verwerkt worden uitbesteedt aan een andere partij, moeten er afspraken worden gemaakt over onder andere de bescherming en verwerking van de persoonsgegevens, welke gegevens er worden verwerkt en voor hoe lang dit gebeurt. Ook moet er vastgelegd worden wat de aard en het doel van de verwerking is en op welke manier de beveiliging van de gegevens is gewaarborgd.

De verwerkersovereenkomst is een overeenkomst die wordt aangegaan door twee partijen; de verwerkingsverantwoordelijke (de gemeente Landsmeer) en de verwerker. De gemeente Landsmeer is verantwoordelijk voor de persoonsgegevens en de verwerker is de 'derde partij' die de verwerking uit handen neemt.

Uit de inventarisatie blijkt dat niet altijd verwerkersovereenkomsten zijn of worden afgesloten met de verwerker. Dit zal dan ook regelmatig onder de aandacht van de verantwoordelijke teammanager gebracht worden. Ondersteuning bij het opstellen en afsluiten van een verwerkersovereenkomst is belegd bij de CISO/PO, FG en de juristen.

3.7 Beveiligingsniveau processen

Niet alle informatie hoeft op hetzelfde niveau beveiligd te worden. De informatie en persoonsgegevens binnen bijvoorbeeld het proces '*informatieverzoek algemeen'* heeft een lagere bescherming nodig dan de informatie en persoonsgegevens binnen het proces '*aanvraag schuldhulpverlening*'. Om de mate van beveiliging van informatie binnen een proces vast te kunnen stellen en de juiste maatregelen te kunnen treffen, moet het beveiligingsniveau bepaald worden. Dit kan door middel van de 'Baselinetoets BBN BIO'. Deze toets kan zowel bij bestaande als bij nieuwe processen ingezet worden en het is de verantwoordelijkheid van de desbetreffende teammanager om deze toets uit te (laten) voeren. De teammanager bepaalt het te beschermen belang en het restrisico wat hij/zij acceptabel vindt. De CISO/PO kan ondersteuning bieden bij het uitvoeren van een baselinetoets.

Het bepalen van het beveiligingsniveau is binnen de gemeente Landsmeer dit jaar uitgevoerd op de volgende processen:

- ✓ Regeling briefadres;
- ✓ Wet BIBOB;
- ✓ Bodycam

Zie voor meer over dit onderwerp ook paragraaf 4.2 'Projecten in 2020' de subparagraaf 'i-Navigator'.

3.8 ENSIA audit

Gemeenten hebben te maken met een steeds groter wordende verantwoordingsplicht wanneer het gaat om Informatiebeveiliging. De Eenduidige Normatiek Single Information Audit (ENSIA) helpt gemeenten hierbij en betekent eenmalige informatieverstrekking en eenmalige IT-audit in plaats van meerdere audittrajecten met verschillende toezichthouders. ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel over informatiebeveiliging en is over het verantwoordingsjaar 2019 gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het ENSIA traject wordt gecoördineerd vanuit de VNG.

ENSIA werkt met een zelfevaluatie methodiek op basis van diverse vragenlijsten. Alle algemene vragen over informatiebeveiliging worden in de BIG zelfevaluatie gesteld. Dit is de grootste vragenlijst uit het stelsel en is ingericht naar de hoofdstukindeling van de tactische baseline BIG. Een deel van de antwoorden wordt gebruikt voor de verantwoording naar de betrokken stelselhouders van het Rijk. Verder zijn er specifieke vragenlijsten voor:

- ✓ DigiD Assessment;
- ✓ Domeinvragen Basisregistratie Adressen en Gebouwen (BAG);
- ✓ Domeinvragen Basisregistratie Grootschalige Topografie (BGT);
- ✓ Domeinvragen Basisregistratie Ondergrond (BRO);
- ✓ Waar staat je gemeente.

Schematische weergave van de vragenlijsten ENSIA 2019

Zelfevaluatie met behulp van diverse vragenlijsten in ENSIA		
BIG zelfevaluatie 2019	**DigiD 2019**	**Specifieke vragenlijsten domeinen 2019**
Informatieveiligheid ▪ Suwinet ▪ BRP ▪ Reisdocumenten ▪ AVG (=BIG)	▪ Aansluiting 1 ▪ Aansluiting 2 ▪ Aansluiting 3 ▪ Etc.	▪ Specifieke vragenlijst BAG ▪ Specifieke vragenlijst BGT ▪ Specifieke vragenlijst BRO ▪ Waarstaatjegemeente (WSJG)

Resultaat ENSIA audit

In 2019 heeft er voor de derde keer een landelijke nulmeting plaatsgevonden naar de mate waarin de BIG bij gemeenten is ingevoerd. Deze meting vindt plaats aan de hand van uitgebreide vragenlijsten. Nieuw in deze audit is de verantwoording over de BRO, voor 2018 is dit een proefjaar geweest en geen verplicht onderdeel van de audit. Gemeenten hebben over 2019 dus voor de eerste keer verantwoording over de BRO moeten afleggen.

Het invullen van de ENSIA zelfevaluatie vragenlijst is conform de landelijke planning voor 31 december 2019 uitgevoerd en aangeboden aan de toezichthouder via het ENSIA portaal. De verdere verantwoording heeft in de loop van 2020 plaatsgevonden. Alle documenten zijn voor de deadline van 1 juni 2020 via het ENSIA portaal geüpload.

Met de collegeverklaring geeft het college van Burgemeester en Wethouders aan in hoeverre de gemeente Landsmeer voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de ENSIA-systematiek. De verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Voor de collegeverklaring wordt u verwezen naar bijlage 1.

De onafhankelijke auditor heeft de collegeverklaring inzake de informatiebeveiliging van DigiD en Suwinet inclusief de bijlagen DigiD en Suwinet onderzocht. Naar het oordeel van de auditor voldoet de gemeente Landsmeer aan in opzet en bestaan aan de beheersingsmaatregelen van de geselecteerde normen van DigiD en Suwinet. De auditor benadrukt dat het om specifieke geselecteerde normen gaat en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel. Voor de volledige rapportage wordt u verwezen naar bijlage 2.

Formeel leidt het beantwoorden van de vragen uit de vragenlijst BIG niet tot een score. Er wordt vanuit de VNG of Rijksoverheid geen percentage opgelegd dat gehaald moet worden. De gemeente Landsmeer kon veel vragen positief beantwoorden. Wel blijkt uit de evaluatie dat bepaalde beveiligingsmaatregelen ad

hoc doorgevoerd worden waarbij geen achterliggend beleid/procedure aanwezig is. Dit zal voor het verantwoordingsjaar 2020 een aandachtspunt zijn.

Resultaten per stelsel
De uitgevoerde zelfevaluaties per stelsel hebben als doel om de procesborging, tijdigheid, volledigheid en juistheid van de data in de basisregistraties te toetsen. De vragenlijsten van de verschillende stelsels leiden wel tot een score. De verschillende rapportages zijn als bijlagen 3 t/m 7 bijgevoegd.

Domein	Score en door te voeren verbeteringen
BRP	De Wet basisregistratie personen (Wbp) schrijft voor dat jaarlijks een onderzoek plaatsvindt naar de procesmatige inrichting, de werking en de beveiliging van de basisregistratie personen (BRP) en naar de inhoudelijke kwaliteit van de gegevens in de BRP. Hiervoor is het gebruik van de 'Kwaliteitsmonitor' voorgeschreven door de Rijksdienst voor Identiteitsgegevens (RvIG). Daarnaast is een deel van dit onderzoek ondergebracht in de ENSIA vragenlijst. De vragenlijst waarmee de procesmatige inrichting, werking en beveiliging van de BRP wordt beoordeeld geeft een totaalscore van 92,8%. De norm voor een voldoende ligt op 90%.
PUN	De Paspoortuitvoeringsregeling (PUN) schrijft voor dat jaarlijks een controle wordt uitgevoerd op de toepassing van beveiligingsmaatregelen en de overige aspecten van het aanvraag- en uitgifteproces van reisdocumenten. Deze controle wordt uitgevoerd op basis van de vragenlijst PNIK zoals opgenomen in de kwaliteitsmonitor van de Rijksdienst voor Identiteitsgegevens (RvIG). De vragenlijst waarmee de procesmatige inrichting, werking en beveiliging van de PUN wordt beoordeeld geeft een totaalscore van 91,3%. De norm voor een voldoende ligt op 90%.
DigiD	Een DigiD-aansluiting dient aan het gehele normenkader van Logius[1] te voldoen. De zelfevaluatie is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan onze leveranciers valt. De overige normen worden afgedekt door een Third Party Mededelingen (TPM) van onze serviceorganisatie Dimpact. Het gaat hierbij om DigiD-aansluiting Digitaal Loket. De uitkomsten uit de zelfevaluatie zijn getoetst door een REgecertificeerde IT-auditor. Deze heeft tevens getoetst of de zelfevaluatie en de TPM van onze serviceorganisatie het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in de Assurance Rapportage met kenmerk 20B0052/MvE/NH. De normen zijn getoetst bij de serviceorganisatie én bij ons en waren alle als voldoende bevonden.

[1] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Zij zorgen voor producten en diensten voor de digitale overheid. Logius biedt voorzieningen en standaarden die alle overheidsorganisaties gebruiken in hun digitale dienstverlening.

BAG	Score gemeente Landsmeer is 93% (landelijke norm is minimaal 75%). De BAG (Basisregistratie Adressen en Gebouwen) bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Uit de zelfevaluatie blijkt dat de gemeente Landsmeer aan de landelijke norm voldoet, wanneer de sub scores bij elkaar opgeteld worden. In de rapportage van de BAG is te lezen dat de gemeente Landsmeer voor het deelaspect tijdigheid onder de landelijke norm scoort. In paragraaf 2.3 worden maatregelen besproken om de score te verbeteren.
BGT	Score gemeente Landsmeer is 90% (landelijke norm is minimaal 75%). De BGT (Basisregistratie Grootschalige Topografie) is de gestandaardiseerde kaart waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd. Uit de zelfevaluatie blijkt dat de gemeente Landsmeer aan de landelijke norm voldoet. In de rapportage van de BGT is te lezen dat de gemeente Landsmeer voor het deelaspect tijdigheid onder de landelijke norm scoort. In paragraaf 2.3 worden maatregelen besproken om de diverse scores te verbeteren.
BRO	Score gemeente Landsmeer is 33,3% (landelijke norm is minimaal 60%). De BRO (Basisregistratie Ondergrond) 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. De gemeente Landsmeer heeft in de eerste zelfevaluatie beneden de landelijke norm gescoord en zal een apart verbeterplan opstellen. Dit verbeterplan zal aan het college aangeboden worden.

Van BIG naar BIO

De BIG is per 1 januari 2020 door de Baseline Informatiebeveiliging Overheid (BIO) vervangen. Er is een grote mate van overlap tussen de BIG en de nieuwe BIO, maar er zijn ook verschillen. De grootste verschillen tussen de beide baselines worden hieronder toegelicht:

- ✓ Anders dan bij de BIG worden binnen de BIO wordt op basis van generieke schade en bedreigingen een onderscheid gemaakt in drie basisbeveiligingsniveaus (BBN's) met bijbehorende beveiligingseisen;
- ✓ Meer risicomanagement. Het management (de proceseigenaar) bepaalt per informatiesysteem het BBN door middel van het uitvoeren van de baselinetoets BBN BIO. Aan de hand van deze toets kan vervolgens het beschermingsniveau en eventuele aanvullende vereisten bepaald worden die nodig zijn om een informatiesysteem te beschermen;
- ✓ Verplichte maatregelen. In de BIO staan de verplichte maatregelen genoemd welke voortvloeien uit wet- en regelgeving. Deze maatregelen vormen de basis voor een betrouwbare en professionele informatievoorziening en zijn daarom -indien van toepassing- allemaal en altijd verplicht voor elke overheidslaag;

- ✓ Toewijzing van maatregelen op eindverantwoordelijke. De maatregelen moeten zijn toegewezen aan een eindverantwoordelijke.

3.9 Beveiligingsincidenten 2019

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen. Een beveiligingsincident kan leiden tot een datalek. De volgende beveiligingsincidenten hebben zich in 2019 voorgedaan:

- ✓ Beeldscherm niet vergrendeld;
- ✓ Openstaande toegangspoortjes van en naar de centrale hal;
- ✓ Ongeautoriseerde toegang tot de kamer van Burgerservice;
- ✓ Persoonsgegevens burger op intranet;
- ✓ Printjes met gevoelige persoonsgegevens onbeheerd bij de printer;
- ✓ Melding zoekgeraakte laptop;
- ✓ Melding phishing mail;
- ✓ Citrix kwetsbaarheid.

3.10 Datalekken 2019

Een beveiligingsincident kan leiden tot een datalek, dit is het geval bij een beveiligingsincident welke per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Bij een datalek is er dus sprake van een inbreuk op persoonsgegevens. Bovengenoemde beveiligingsincidenten kunnen als een datalek aangemerkt worden:

- ✓ Persoonsgegevens burger op intranet;
- ✓ Printjes met gevoelige persoonsgegevens onbeheerd bij de printer.

Een ernstig datalek moet binnen 72 uur nadat het datalek ontdekt is, gemeld worden aan de Autoriteit Persoonsgegevens (AP). Wanneer er een hoog risico bestaat voor de rechten en vrijheden van de betrokken personen, moet dit bij de betrokken personen gemeld worden. Geen van de gemelde/ontdekte datalekken was van dusdanige aard dat de AP of betrokkenen hierover ingelicht dienden te worden.

3.11 Privacyverklaring

Gemeenten hebben een informatieplicht wat betreft de verwerking van persoonsgegevens. Dat betekent dat de gemeente Landsmeer verplicht is om inwoners en andere betrokkenen duidelijk te informeren over wat de gemeente Landsmeer met hun persoonsgegevens doet en waarom. In de praktijk is een online privacyverklaring de meest handige manier om hier aan te voldoen. Op de homepage van de gemeentelijke website is de privacyverklaring makkelijk vindbaar.

3.12 Data Protection Impact Assessment (DPIA)

Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. In de Nederlandse vertaling van de Algemene Verordening Gegevensbescherming (AVG) wordt de term Data Protection Impact Assessment (DPIA) 'gegevensbeschermingseffectbeoordeling' genoemd. Het uitvoeren van een DPIA geldt sinds de inwerktreding van de AVG.

Organisaties hoeven niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Daarnaast heeft de Autoriteit Persoonsgegevens (AP) een lijst van verwerkingen opgesteld waarvoor een DPIA verplicht is.

Binnen de gemeente Landsmeer is dit jaar voor de volgende processen een DPIA uitgevoerd:

- ✓ Bodycams voor BOA's

3.13 Conclusie

Voor zowel informatiebeveiliging als de privacy is beleid opgesteld, zodat de kaders duidelijk afgebakend zijn en de verantwoordelijkheden binnen de organisatie belegd.

Omdat door omstandigheden al ruim een half jaar (eerste helft van 2019) geen aandacht is geweest voor informatiebeveiliging en privacy, is de kennis over dit onderwerp erg laag binnen de organisatie. Op verschillende manieren wordt getracht de bewustwording van de medewerkers en de teammanagers te vergroten.

Door het uitvoeren van een audit voor de informatiebeveiliging en een nulmeting voor de privacy, zijn de 'pijnpunten' voor de gemeente Landsmeer in kaart gebracht. Dit heeft voor de AVG een implementatieplan opgeleverd met een duidelijke planning en een overzicht van de stand van zaken. Voor informatiebeveiliging zijn de uitkomsten van de ENSIA aangehouden om de stand van zaken inzichtelijk te krijgen.

Conclusie van de ENSIA audit is dat er aandacht is voor informatieveiligheid binnen de gemeentelijke processen, maar dat maatregelen soms op een ad hoc basis worden doorgevoerd. Quick wins kunnen voor 2020 behaald worden door beleid en/of procedures op te stellen zodat maatregelen niet op een ad hoc basis worden toegepast maar door een weloverwogen keuze.

Er is een beveiligingsincidenten- en datalekregister opgesteld waarin de meldingen worden bijgehouden. Hier wordt ook vermeld welke acties zijn/worden genomen om herhaling te voorkomen.

Een voorzichtig begin is gemaakt met het uitvoeren van risicoanalyses voor nieuwe processen en -wanneer uit de analyse blijkt dat er een verhoogd privacy risico is binnen het proces- het uitvoeren van een DPIA.

4 Doorkijk naar 2020

In dit hoofdstuk wordt eerst een tweetal gebeurtenissen besproken welke impact hebben (gehad) op onze informatiebeveiliging. Daarnaast blikken we vooruit naar 2020 en welke activiteiten en werkzaamheden uitgevoerd gaan worden om de beveiliging van bedrijfsinformatie en (persoons)gegevens verder te verbeteren.

4.1 Gebeurtenissen met grote impact op de informatieveiligheid en privacy

Begin 2020 heeft een tweetal gebeurtenissen plaatsgevonden met grote invloed op de informatieveiligheid en de privacy.

Beveiligingsincident Citrix

Eind december 2019 heeft een ernstig beveiligingsincident plaatsgevonden binnen Citrix Netscaler. Misbruik van de kwetsbaarheid zou kwaadwillenden in staat stellen om directe toegang te verkrijgen tot het lokale netwerk en systemen. De Informatiebeveiligingsdienst (IBD) heeft op basis van deze informatie het beveiligingsincident ingeschaald op High/High. Er is constant nauw contact onderhouden tussen KPN Werkplek, de Teammanager Ondersteuning, de systeembeheerder, de CISO, de secretaris en de burgemeester. Er is door de CISO een draaiboek opgesteld waarin de mogelijke consequenties van het stil laten leggen van Citrix voor de bedrijfsvoering van gemeente Landsmeer wordt beschreven, evenals de mogelijke gevolgen voor de bedrijfsvoering van gemeente Landsmeer wanneer partners hun Citrix stil (laten) leggen of hebben stilgelegd. Daarnaast bevat dit draaiboek een aantal acties die gemeente Landsmeer moet ondernemen wanneer Citrix daadwerkelijk zou worden stilgelegd.
Omstreeks half januari gaven de Informatiebeveiligingsdienst (IBD) en de Nationaal Cyber Security Centrum (NCSC) het advies om – wanneer niet voor 8 januari de mitigerende maatregelen genomen waren – Citrix stil te leggen. De gemeente Landsmeer heeft na een weloverwogen keuze besloten om de Citrix niet stil te laten leggen. Van het incident is een volledig verslag met conclusies door de CISO opgesteld.

Coronacrisis

In het eerste kwartaal van 2020 breekt ook in Nederland het Coronavirus uit. Alle medewerkers van de gemeente Landsmeer kregen op donderdag 12 maart te horen dat ze -indien mogelijk- thuis moesten gaan werken. Dit heeft uiteraard verregaande consequenties, ook op het gebied van informatieveiligheid en privacy.
Via intranet is voorlichting gegeven hoe bij thuiswerken op een veilige manier met bedrijfsinformatie en persoonsgegevens gewerkt kan worden.
Door het thuiswerken is het noodzakelijk dat de mogelijkheid tot digitaal vergaderen gefaciliteerd wordt. Team Automatisering heeft dan ook versneld Microsoft Teams uitgerold om in deze behoefte te voorzien. Er is een protocol '*videobellen en online vergaderen*' door de CISO opgesteld en ter goedkeuring voorgelegd aan het TMO en de OR. Dit protocol is op 12 mei vastgesteld door het college. Dit protocol is onder de aandacht gebracht via intranet en de teammanagers hebben daarnaast hun medewerkers ook op dit protocol gewezen.

4.2 Projecten in 2020

In 2020 is een aantal projecten gepland waarmee de (inrichting van) de informatieveiligheid en privacy verder ontwikkeld wordt en de organisatie meer grip kan krijgen op de informatieveiligheid en privacy binnen de werkprocessen.

i-Navigator

De i-Navigator is een tool waarmee de complete informatiehuishouding van de organisatie centraal in kaart gebracht wordt en beheerd kan worden.
In de i-Navigator worden de werkprocessen, de informatieobjecten die een rol spelen bij die werkprocessen, de basis- en kernregistraties die worden geraadpleegd binnen de werkprocessen en de informatiesystemen waarin deze registraties worden beheerd, beschreven.

Verwerkingsregister

Vanuit de AVG is de verplichting gesteld tot het hebben en onderhouden van een verwerkingsregister. Iedere organisatie die gegevens verwerkt moet bijhouden welke persoonsgegevens zij verwerkt, voor welk doel, van welke categorieën betrokkenen, wie de ontvangers zijn, et cetera. Het opstellen van een verwerkingsregister geeft inzicht in de verwerkingsactiviteiten binnen de organisatie. Bovendien is het verwerkingsregister één van de middelen om aan te tonen dat er voldaan wordt aan de basisbeginselen van privacy, wat een andere verplichting is uit de AVG. Binnen de i-Navigator is een standaard verwerkingsregister opgesteld. Per werkproces is namelijk alle informatie vastgelegd die thuishoren in een verwerkingsregister. De gemeente Landsmeer kan -wanneer nodig- het verwerkingsregister aanpassen aan haar eigen situatie.

Basisbeveiligingsniveau (BBN)

Informatiebeveiliging is risicomanagement. Dit betekent dat de teammanagers voor hun processen het basisbeveiligingsniveau (BBN) moeten bepalen. Hierbij wordt gekeken naar het risico op mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Afhankelijk van de hoogte van de toegekende BBN (BBN 1, 2 of 3), leidt dit tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken zullen passende maatregelen moeten worden getroffen of wordt het (rest)risico geaccepteerd. In de i-Navigator staat per werkproces al het BBN vermeld. De verantwoordelijke teammanager kan -wanneer nodig- het BBN (laten) aanpassen wanneer uit een Baselinetoets BBN BIO naar voren komt dat het werkproces een afwijkende BBN heeft.

Information Security Management System (ISMS)

De BIO geeft aan dat gemeenten moeten beschikken over een ISMS. Een ISMS is een procesgerichte benadering voor informatiebeveiliging en privacy en volgt de plan-do-check-act cyclus. Zoals gezegd is het ISMS een proces en geen tool. Wel zijn er tools op de markt welke het ISMS kunnen ondersteunen en de gemeente Landsmeer heeft gekozen voor Recourse. Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het helpt de gemeenten onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid en de kwaliteit van de informatievoorziening en bedrijfscontinuïteit te waarborgen. In 2020 zal gestart worden met de inrichting van de tool Recourse.



Security Information & Event Management (SIEM) en Security Operations Center (SOC)

Een andere eis die de BIO stelt (onder hoofdstuk 12 'verslaglegging en monitoren'), is het gebruik van SIEM en SOC om de digitale weerbaarheid bij gemeenten te verhogen. De combinatie van SIEM en SOC draagt er toe bij dat computerdreigingen zoals hackpogingen en malware, beter worden gemonitord en in kaart worden gebracht en dreigingen en aanvallen in een zeer vroeg stadium gedetecteerd kunnen worden. Op basis van deze vroegtijdige detectie kan er actie ondernomen worden om de aanval zo snel mogelijk te stoppen of in een aantal gevallen zelfs te voorkomen. GGI-Veilig heeft namens een groot aantal gemeenten en gemeentelijke samenwerkingsverbanden een openbare Europese aanbesteding verzorgd om het gewenste producten- en dienstenportfolio te verwerven. Deze aanbesteding heeft geleid tot raamovereenkomsten, waar deelnemende gemeenten gebruik van kunnen maken. De aanbesteding SIEM SOC (perceel 1) is gegund aan KPN. De gemeente Landsmeer heeft de eerste oriënterende gesprekken met KPN gevoerd.

4.3 Overige activiteiten en werkzaamheden in 2020

Naast bovengenoemde projecten zal er ook aandacht zijn voor overige activiteiten en werkzaamheden in 2020. Niet alleen het verder uitwerken van activiteiten en werkzaamheden die in 2019 aangevangen zijn, maar ook nieuwe activiteiten en werkzaamheden.

Informatiebeveiliging en privacy binnen het inkoopproces

Binnen het huidige inkoop- en aanbestedingsproces is er te weinig aandacht voor informatiebeveiliging en privacy. Vaak worden de voorwaarden voor informatiebeveiliging en privacy door de leverancier beschreven en door ons geaccepteerd. Op dat gebied moet de organisatie meer 'in control' komen door bij een inkoop- of aanbestedingstraject zelf eisen te formuleren op het gebied van informatiebeveiliging en privacy. De CISO/PO gaat met de gemeentelijke inkoper in gesprek hoe informatiebeveiliging en privacy onderdeel kan gaan uitmaken van een inkoop- of aanbestedingstraject.

Diverse protocollen en procedures
Ter ondersteuning van ons werk wordt in 2020 diverse protocollen en procedures opgesteld. Dit om goed in beeld te hebben welke afspraken er gelden en wat er van welke medewerker verwacht wordt en hoe eventueel de verantwoordelijkheden belegd zijn. Protocollen/procedures die dit jaar opgesteld en vastgesteld worden:

- ✓ Procedure 'Rechten van betrokkenen';
- ✓ Procedure 'Meldplicht datalekken';
- ✓ Protocol 'Gedragscode Informatiebeveiliging en Privacy'.

Nulmeting informatiebeveiliging
Dit jaar zal een nulmeting uitgevoerd worden gericht op de stand van zaken wat betreft informatieveiligheid. Hiervoor zal gebruik gemaakt worden van de GAP-analyse BIO. Het bedrijf Sincerus zal ondersteuning bieden bij het afnemen van de interviews binnen de organisatie. Aan de hand van de uitkomsten wordt een Informatiebeveiligingsplan opgesteld. Doelstelling van dit document is het geven van inzicht in de actuele maatregelen, procedures en processen welke zijn geïmplementeerd om de kwaliteit van de informatieveiligheid te waarborgen. Daarnaast worden in dit plan ook verbeteracties benoemd, de eigenaar van elke verbeteractie en een planning wanneer welke verbeteractie wordt doorgevoerd.

Nulmeting Privacy
De nulmeting staat voor eind juni 2020 gepland en kan vergeleken worden met de nulmeting uit 2019 om te inventariseren welke maatregelen afgelopen jaar zijn doorgevoerd.

ENSIA audit
Ook dit jaar start per 1 juli de nieuwe cyclus voor uitvoering van de zelfevaluatie informatiebeveiliging. Met ENSIA krijgt het college meer inzicht in de stand van zaken van de informatieveiligheid en kan beter sturen op informatieveiligheid. Het college legt verantwoording over de informatieveiligheid af aan de gemeenteraad.

Bewustwording
In 2019 is een begin gemaakt met het vergroten van de bewustwording voor informatieveiligheid en privacy bij zowel de medewerkers als bij de teammanagers.

Aandacht voor het vergroten van de bewustwording zal ook dit jaar op de agenda staan. Dit zal op een andere manier aangepakt moeten worden; door de coronacrisis is het onmogelijk om voor (grote) groepen bijeenkomsten te organiseren. Daarbij komt dat de medewerkers zo veel mogelijk thuis aan het werk zijn. De mogelijkheid wordt nu onderzocht om een online trainingsprogramma aan te bieden. Het creëren van bewustwording is geen éénmalige actie, maar een continu proces. Een online trainingsprogramma is hiervoor uitermate geschikt, omdat de lesstof periodiek uitgerold kan worden. De medewerkers kunnen de lesstof volgen op het moment dat het hun het beste schikt of dit nu op hun telefoon, i-pad of laptop is.