

## Rapportage ENSIA informatiebeveiliging & privacy 2018

### 1. Inleiding

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten eenvoudiger te maken. Uitgangspunt van ENSIA is *de single information audit*. Dit betekent dat we maar één keer per jaar een zelfevaluatie op het gebied van informatiebeveiliging uitvoeren. Diverse bewijsstukken moeten daarbij vastgelegd worden en er vindt gedeeltelijk controle plaats door een externe IT auditor. Deze informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting ministeries. Aan deze rapportage is een (niet verplicht) onderdeel over privacy toegevoegd.

ENSIA richt zich op de volgende onderdelen:

#### 1. Basisregistraties waar de gemeente bronhouder van is:

- Basisregistratie Personen (BRP);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Grootschalige Topografie (BGT).

#### 2. Kritische processen:

- Suwinet;
- Paspoorten, ID-kaarten en rijbewijzen;
- DigiD (2 aansluitingen).

#### 3. Baseline Informatiebeveiliging Gemeenten (BIG)

### 2. Aan wie leggen we verantwoording af?

Horizontaal:

- Concernteam;
- College van burgemeester en wethouders;
- Gemeenteraad.

Verticaal:

- Ministerie van Sociale zaken (BKWI inzake Suwinet);
- Ministerie BZK (RvIG inzake paspoorten, ID-kaarten en rijbewijzen);
- Ministerie BZK (Logius inzake DigiD-aansluitingen);
- Ministerie BZK (Inzake de BRP);
- Ministerie Infrastructuur en Waterstaat (BAG en BGT).

### 3. Stappen in het verantwoordingsproces

- Uitvoeren zelfevaluaties.
- Opstellen collegeverklaring: de collegeverklaring is opgesteld op basis van bevindingen uit onze zelfevaluatie op Suwinet en DigiD. Hierin verklaart het college dat de zelfevaluatie naar eer en geweten ingevuld is en dat eventuele tekortkomingen in verbeterplannen zijn opgenomen.
- Een externe IT auditor toetst deze collegeverklaring en neemt de bevindingen op in een assurancerapport. Met de vastgestelde collegeverklaring en het assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

#### 4. Samenvattend beeld collegeverklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Twenterand op 31 december 2018 voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen. Het gaat concreet om 2 DigiD aansluitingen (iBurgerzaken en de website) en de aansluiting op Suwinet. We voldoen aan alle normen, waardoor een verbeterplan niet nodig is. Hieronder volgt een samenvattend beeld:

| Onderdeel                    | Wordt aan alle geselecteerde normen voldaan? | Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord? |
|------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| DigiD 503787                 | Ja                                           | Neen                                                                                                                         |
| DigiD 1001861                | Ja                                           | Neen                                                                                                                         |
| Suwinet voor SUWI-taken      | Ja                                           | Neen                                                                                                                         |
| Suwinet voor niet-SUWI-taken | Ja                                           | Neen                                                                                                                         |

#### 5. Informatiebeveiliging 2018

De doelstelling van informatiebeveiliging is als volgt: het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie(systemen) van onze gemeente. Dit onderwerp wordt steeds belangrijker omdat we informatiegestuurd en datagedreven werken. Zonder een adequate beveiliging van onze 'kroonjuwelen' kunnen we als Twenterand niet functioneren: persoonsgegevens, financiële- en medische gegevens, vertrouwelijke plannen en kritieke systemen. Hoe we onze informatiebeveiliging organiseren is niet geheel vrijblijvend. Alle gemeenten in Nederland hebben zich namelijk geconformeerd aan een norm voor informatiebeveiliging: de Baseline Informatiebeveiliging Gemeenten (BIG).

De BIG is een normenkader, bestaande uit 302 maatregelen, met betrekking tot informatiebeveiliging. In 2017 is gestart met het prioriteren van de maatregelen (hoog, midden en laag). Sindsdien zijn verschillende maatregelen genomen. Denk bijvoorbeeld aan:

- gemeentebreed informatiebeveiligingsbeleid;
- wachtwoordbeleid;
- verschillende bewustwordingsactiviteiten (phishingtests, mystery guest, presentaties);
- beleid omtrent het melden en oplossen van beveiligingsincidenten;
- geheimhoudingsovereenkomsten voor nieuwe medewerkers;
- clear screen en clear desk beleid.

#### 6. Privacy 2018

2018 stond vooral in het teken van de bescherming van persoonsgegevens. Dit natuurlijk door de komst van de Algemene Verordening Gegevensbescherming (AVG). Deze is sinds 25 mei van toepassing. In 2018 is dan ook voornamelijk aandacht besteed aan het voldoen aan de eisen die deze wetgeving stelt. De basisvoorwaarden zijn inmiddels ingericht. Denk hierbij aan het:

- gemeentebreed privacybeleid;
- benoemen van een interne toezichthouder, de functionaris gegevensbescherming (FG);
- inrichten van een proces omtrent het melden van beveiligingsincidenten en (mogelijke) datalekken;
- opstellen van een register van verwerkingsactiviteiten;
- sluiten van verwerkersovereenkomsten met derde partijen;
- informeren van inwoners middels een privacyverklaring op de website;
- inrichten van een proces omtrent de rechten van 'betrokkenen' (bijvoorbeeld inzagerecht);
- uitvoeren van privacy impact assessment (PIA's).

## **7. Beveiligingsincidenten en datalekken in 2018**

100% beveiligen van informatie bestaat niet. Het is daarom van belang dat we goed omgaan met beveiligingsincidenten. Als er bij een beveiligingsincident persoonsgegevens betrokken zijn spreken we van een datalek. Een 'ernstig' datalek dienen we te melden bij de Autoriteit Persoonsgegevens en/of aan de betrokkenen wie het betreft. Een datalek kan als ernstig worden gekwalificeerd indien er persoonsgegevens van gevoelige aard zijn gelekt (denk aan Burgerservicenummers en gezondheidsgegevens). Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Dit wordt altijd per incident onderzocht.

We onderschrijven het belang van een adequate behandeling van incidenten en de response daarop om daarmee de gevolgen voor de bedrijfsvoering te minimaliseren. Dit begint bij het registreren van alle incidenten die plaatsvinden. Elke medewerker dient alert te zijn op bedreigingen en kwetsbaarheden met betrekking tot informatiebeveiliging en privacy en is verplicht om elk beveiligingsincident intern te melden dat hij/zij ontdekt of vermoedt.

In 2018 zijn er 10 beveiligingsincidenten intern geregistreerd, waaronder 6 datalekken. Het ging hierbij onder andere om incidenten waarbij e-mails per ongeluk naar de verkeerde ontvanger zijn verstuurd of vertrouwelijke informatie op een andere manier (mogelijk) toegankelijk was voor onbevoegden. Alle gemelde incidenten zijn geanalyseerd en gedocumenteerd en waar nodig, conform de AVG, gemeld aan de Autoriteit Persoonsgegevens.

Door de continue aandacht voor dit onderwerp wordt de bewustwording binnen de gehele organisatie verhoogd. De verwachting is dat (mogelijke) incidenten daardoor vaker en sneller herkend worden, met als gevolg dat er intern meer incidentmeldingen zullen worden gedaan.

## **8. Informatiebeveiliging & privacy in 2019**

De AVG zal in 2019 verder geïmplementeerd worden. Extra aandacht zal hierbij worden besteed aan het sociaal domein. De gevoeligheid van de gegevens en de vele ketenpartners die hierbij betrokken zijn maken een goede omgang met persoonsgegevens gecompliceerd.

Voor wat betreft de informatiebeveiliging zal in 2019 de focus komen te liggen op de implementatie van een nieuwe norm. Zoals eerder genoemd hanteren gemeenten tot nu toe de BIG als normenkader. Ook het Rijk, de waterschappen en provincies hanteren hun eigen respectievelijke normen. Deze normen worden gebundeld in één gezamenlijk normenkader: de Baseline Informatiebeveiliging Overheid (BIO). De BIO wordt op 1 januari 2020 van kracht. Ter voorbereiding hierop zullen we in 2019 al zoveel mogelijk uitgaan van de BIO.

Een aantal voorbeelden van maatregelen die genomen zullen worden:

1. Technische / fysieke maatregelen:
  - goede scheiding tussen publieksruimte en werkruimte
  - invoering twee-factor-authenticatie;
  - wijzigingsbeheer, back-up en recovery.
2. Procesmatige maatregelen:
  - inrichten proces omtrent autorisatiemanagement (logische toegangsbeveiliging);
  - inrichten proces omtrent fysieke toegangsbeveiliging (waaronder bezoekersregeling);
  - beleid voor mobiele apparatuur en telewerken.
3. Mensen:
  - gepersonaliseerde toegangspassen;
  - bewustwording: nanolearning over informatiebeveiliging.

De wereld om ons heen blijft veranderen en de techniek blijft zich verder ontwikkelen. Dus ook bedreigingen en risico's veranderen constant. Informatiebeveiliging en privacy vereisen daarom onze continue aandacht.