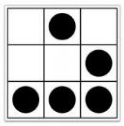
BELEID INFORMATIEVEILIGHEID

Gemeente Zeist

Weerbaar verder…



Documentcode:	0309287 Bijlage 1. bij collegevoorstel 272306 Weerbaar verder
Versie	1.0
Versiedatum	5 februari 2019
Gemaakt door:	A. van Leeuwen
Goedgekeurd door	College van B&W
V-Classificatie	Intern document / openbaar

Symbool op voorpagina

is een weergave van een 'Glider'. Een glider is een patroon in de Game of Life van de Britse wiskundige en professor John Conway, dat zich voortbeweegt over het raster (grid). Het is ontdekt door de Britse wiskundige en hoogleraar Richard Guy. Het is het kleinste voortbewegende patroon (ook spaceship genoemd) in de Game of Life. Om de vier iteraties heeft het patroon zich 1 cel verplaatst over het grid. De glider ontstaat vaak uit willekeurige configuraties (toestanden) van de cellulaire automaat.

Gliders zijn van belang in de Game of Life aangezien ze gemakkelijk te maken zijn, ze kunnen andere patronen raken om meer complexe patronen te produceren en ze kunnen worden gebruikt om informatie te versturen over grote afstanden.

De Amerikaanse programmeur en publicist Eric Raymond heeft het patroon voorgesteld als symbool voor hackers, aangezien:

- *de glider rond dezelfde tijd is ontstaan als Unix en internet*
- *de Game of Life de interesse wekte van hackers.*

Het symbool is daarna door de (goedwillende) internationale hackers gemeenschap geadopteerd als hun' logo. Het staat daarmee impliciet voor informatieveiligheid: wees bewust van het feit dat er altijd een (onbedoelde) ingang of uitgang kan zijn in onze systemen.

Versie gegevens

Datum	Versie	Omschrijving van de aanpassing
16-10-2018	0.1	Aangepaste versie Nieuwegein nav Zeister beleid 2016-2018
01-11-2018	0.7	Conform BIG en met Nieuwgein afgestemd
12-12-2018	0.9	Aanscherping nav interne meelees ronde
06-02-2019	0.95	Aanscherping nav bespreking GMT en wethouder
12-02-2019	1.0	Definitief

Inhoudsopgave

1. Inleiding en samenvatting

1.1. Inleiding

Voor u ligt het ***Beleid Informatieveiligheid 2019 Weerbaarder verder….*** van de gemeente Zeist waarin onder meer de kaders, uitgangspunten, verantwoordelijkheden en richting om Informatieveiligheid structureel te borgen in de gemeentelijke organisatie zijn vastgelegd. In dit document wordt bewust gesproken van Informatieveiligheid en niet over Informatiebeveiliging. Het gaat om het intrinsieke begrip 'veiligheid van' en niet het mechanistische 'beveiligen van'.

> *Informatieveiligheid is geen doel op zich, maar moet de primaire bedrijfsprocessen ondersteunen en de veilige en verantwoorde uitvoering daarvan mogelijk maken. Informatieveiligheid dient dus vanuit het primaire proces gestuurd te worden, daar waar het eigenaarschap van de informatie ligt*.

Informatieveiligheid is erop gericht vertrouwelijke informatie afdoende te beschermen tegen misbruik of ongeautoriseerde toegang, maar ook om de beschikbaarheid en integriteit van de informatie en daaraan verbonden dienstverlening te blijven garanderen. Een overheid die informatieveiligheid niet omarmt, verliest het vertrouwen van de burger en daarmee haar legitimiteit.
De VNG heeft eind 2013 het belang van Informatieveiligheid benadrukt door in een algemene ledenvergadering een resolutie te bekrachtigen waarin staat dat informatieveiligheid wordt opgenomen in de portefeuille van een van de leden van het college van burgemeester en wethouders (B&W) en dat de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) het gemeentelijke basisnormenkader voor informatieveiligheid wordt. In deze resolutie is ook aangegeven dat gemeentes de informatieveiligheid zowel bestuurlijk als organisatorisch borgen en deze transparant maken voor burgers, bedrijven en (keten)partners.

Een andere ontwikkeling waarin het belang van Informatieveiligheid tot uiting komt, is de komst van de Algemene Verordening Gegevensbescherming (AVG). Deze uniforme Europese regelgeving is er op gericht dat elke organisatie privacy van burgers als groot goed omarmt en borgt. Informatieveiligheid is hiermee nauw verbonden.

Reden te meer om Informatieveiligheid structureel te borgen in de organisatie. Dit beleidsdocument is normstellend en biedt daarvoor de basis. Centraal ligt de nadruk op het realiseren van een ISMS wat staat voor een Information Security Management System ofwel een informatie beveiligingsmanagementsysteem. Dat bestaat uit twee delen:
Allereerst is daar het gedachtengoed dat daarachter steekt, waarbij op bestuurlijk niveau op voortgang en verbetering van Informatieveiligheid wordt gestuurd. De leiding hanteert daarbij het model van Plan-Do-Check-Act als continue verbetercyclus. ISMS is als het ware de 'motor', een proces dat zorgdraagt voor de periodieke planning, implementatie, onderhoud, beoordeling en het verder verbeteren van de Informatieveiligheid als resultante van dat proces binnen de context van de gemeente. Zie ook paragraaf 4.3.
Het tweede deel is de bewaking van de Administratieve Organisatie in dezen. In een ISMS als softwaresysteem wordt de complexe stand van zaken (processen, documentatie, voortgang, evaluaties, etc.) bijgehouden om het overzicht op alle geplande en gerealiseerde dan wel (nog) niet gerealiseerde verbeteringen bij te kunnen houden.

Met ISMS als denkwijze en als systeem is de gemeente beter in staat om Informatieveiligheid te managen, bedrijfsmiddelen te beschermen, de bewustwording en acceptatie van Informatieveiligheid bij medewerkers te versterken, ongeautoriseerde toegang tot informatie te voorkomen, snel en

adequaat te kunnen reageren op veiligheidsincidenten, persoonsgegevens van burgers en medewerkers te beschermen, de bedrijfscontinuïteit te garanderen en te voldoen aan naleving van wet- en regelgeving.

1.2. Samenvatting

Het college van B&W en het management spelen een cruciale rol bij het uitvoeren van dit Informatieveiligheidsbeleid. Het college van B&W geeft een duidelijke richting aan Informatieveiligheid en demonstreert dat zij Informatieveiligheid ondersteunt en zich hierbij betrokken voelt door het vaststellen en uitbrengen van Informatieveiligheidsbeleid voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). De uitwerking van dit beleid naar de organisatie ligt bij het management. Het management stuurt op risico's, bepaalt welke veiligheidsmaatregelen nodig zijn, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Het management wordt hierbij ondersteund door de Chief Information Security Officer (CISO).
De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hierbij geldt dat:

- er wet- en regelgeving is waar altijd aan voldaan moet worden, zoals niet uitputtend, onder andere de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), SUWInet DigiD, Basisregistratie Adressen en gebouwen (BAG), maar ook de Archiefwet en de Algemene Verordening Gegevensbescherming (AVG) Zie hiervoor verder hoofdstuk 6;
- een gemeenschappelijk normenkader voor Informatieveiligheid als basis dient, te weten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
- de gemeente dit normenkader vaststelt waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe;
- er een proces op bestuurlijk en uitvoerend niveau is van continue verbetering in het borgen van Informatieveiligheid (plan – do – check – act).

Een belangrijke toevoeging aan dit beleid is dat er vanaf nu wordt gestreefd om het Informatieveiligheidsbeleid van de gemeentes Zeist en Nieuwegein inhoudelijk af te stemmen en synchroon te laten lopen. De gemeentes hebben met de gezamenlijke aanschaf van een nieuwe ICT infrastructuur (datacenter) impliciet de basis gelegd voor onderlinge afstemming over het volgen van de vereisten uit de BIG.
Dit aangescherpte beleid is een vervolg op de eerdere beleidsnota's Informatieveiligheid[1].

[1] *Weerbaarheid als basis: bewustzijn als actieve prikkel. 13cv00472 & Weerbaar en Bewust 16cv00337)*

2. Informatieveiligheid

2.1. Definitie van Informatieveiligheid

Informatieveiligheid is het samenhangend stelsel van beheersingsmaatregelen dat de **B**eschikbaarheid / continuïteit, de **I**ntegriteit / betrouwbaarheid en **V**ertrouwelijkheid / exclusiviteit van de informatie garandeert (BIV). Daar waar gesproken wordt over informatie geldt dit ook voor de onderliggende gegevens.
Het begrip Informatieveiligheid heeft aldus betrekking op:

- **B**eschikbaarheid / continuïteit: zorgen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- **I**ntegriteit / betrouwbaarheid: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- **V**ertrouwelijkheid / exclusiviteit: beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

2.2. Het belang van Informatie(veiligheid) beleid

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

Het Informatieveiligheidsbeleid is het kader voor passende bestuurlijke, technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving en het vertrouwen van haar klanten waardig is. De gemeente streeft ernaar om aantoonbaar ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control zijn betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn, dat er een planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de plan-do-check-act cyclus (PDCA-cyclus), aangestuurd door een ISMS systeem.
Het college van B&W, managementteam (GMT) en lijnmanagement (BMO) dragen de inhoud uit naar alle medewerkers en gebruikers die zijn betrokken bij de verwerking en beheer van informatie en/of het beheer van informatiesystemen, waarvoor de verantwoordelijkheid bij de gemeente ligt. Het Informatieveiligheidsbeleid is van toepassing op alle medewerkers en gebruikers van informatie.

2.3. Kaders Informatieveiligheid en privacy

De komende jaren zet de gemeente in op het verhogen van Informatieveiligheid en verdere professionalisering van de Informatieveiligheidsfunctie 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. Dit vereist een integrale, open en transparante aanpakgoed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel dient hierbij te worden betrokken en zich actief op te stellen.

Een integraal onderdeel van de Informatieveiligheid is privacy; een bestaand iets, maar in de afgelopen jaren, mede door de digitalisering en brede uitwisseling (ketensamenwerking) van informatie en de AVG (Europese wetgeving), als opvolger van de Wet Bescherming

persoonsgegevens (WBP) veel actueler geworden. Het raakt de persoonlijke levenssfeer van burgers en vereist een andere houding en invulling van het omgaan met gegevens door de overheid. Want gemeentes zijn niet alleen verantwoordelijk voor het borgen van de privacy van hun inwoners, maar ook deels voor het zorgvuldig omgaan met persoonsgegevens in de ketens die zij regisseren en de netwerken waarin ze samenwerken. Daarbij is het van belang om te weten waar ieders verantwoordelijkheid begint en eindigt.

Vanuit dit oogpunt is het noodzakelijk een visie op privacy en privacy beleid te formuleren, zodat deze gebruikt kan worden als kapstok om de uitvoering ervan, zoals de regie op eigen gegevens, vorm te geven. Daarbij is het kunnen voldoen aan de AVG het uitgangspunt.
In 2016 is er reeds een visie op privacy vastgesteld. Nu met de komst van de AVG kan niet langer worden volstaan met privacy opnemen in het (brede) Informatieveiligheidsbeleid, daarom wordt er tevens een separaat privacy beleid opgesteld.

2.4. Visie op Informatieveiligheid

De visie op informatieveiligheid luidt als volgt:

> *De gemeente zet structureel in op het verhogen van Informatieveiligheid en verdere professionalisering van de informatieveiligheidsfunctie 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. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel en alle medewerkers zijn hierbij betrokken.*

Het proces van Informatieveiligheid is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een ‘ katalysator; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus ligt daarbij op informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

2.5. Beleidsprincipes Informatieveiligheid

De hieronder genoemde beleidsprincipes gelden als uitgangspunt bij het verder ontwikkelen van maatregelen, spelregels en afspraken rondom de informatieveiligheid van de gemeente. De principes volgen in grote lijnen de veiligheidscategorieën uit de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- **Informatieveiligheid zit in ons DNA** (informatieveiligheidsbeleid)
  De klassieke aanpak inzake informatieveiligheid waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig faciliteren. Informatieveiligheid is op een natuurlijke manier ingebed in de activiteiten van de organisatie en het handelen van de medewerkers.

- **Aansluiten op bestaande standaarden** (informatieveiligheidsbeleid)
  Waar mogelijk wordt bij de realisatie van de Informatieveiligheid gebruik gemaakt van (landelijke) standaarden of veelgebruikte, bewezen oplossingen.

- **Informatieveiligheid is van iedereen** (personeel)
  Informatieveiligheid is een integraal onderdeel van het proces en hoort bij de taken en

verantwoordelijkheden van elke manager en medewerker. Bewustzijn en zorgvuldig handelen zijn de belangrijkste veiligheidsmaatregelen.

- **De gemeente blijft eindverantwoordelijk** (computer- en netwerkbeheer)
  De gemeente voert de regie over de dienstverlening. Met alle samenwerkingspartners maakt de gemeente afspraken over de beschikbaarheid, de integriteit en de vertrouwelijkheid van de onderlinge informatiestromen. Samenwerkingspartners die zich niet kunnen of willen conformeren aan het normenkader kunnen niet aansluiten op de basisinfrastructuur van de gemeente.

- **Incidenten worden gemeld** (beheer van informatieveiligheidsincidenten)
  Elk incident op het gebied van Informatieveiligheid wordt ten minste gemeld aan de procesverantwoordelijke. Deze rapporteert over de incidenten in de Planning & Control cyclus. Het incidentenregister wordt gebruikt om trends te signaleren en dient als input bij de revisie van het veiligheidsplan. De gemeente trekt lering uit incidenten.

- **Privacy en vertrouwelijke informatie** (naleving)
  De medewerkers van de gemeente gaan integer om met privacygevoelige gegevens en vertrouwelijke informatie. Je hebt alleen toegang tot informatie die voor jou relevant is of nodig is om je werk uit te voeren. Persoonsgegevens worden adequaat beveiligd. Dit wordt getoetst.

- **Wettelijke verplichtingen en auteursrechtelijk beschermd materiaal** (naleving)
  De gemeente draagt er zorg voor dat medewerkers op de hoogte zijn van de informatieveiligheidsaspecten binnen hun proces(sen) en dat de gemeente niet in strijd met wet- en regelgeving handelt. Dit wordt operationeel ondersteund door de Eenduidige Normatiek Single Information Audit (ENSIA). Zie ook hoofdstuk 5.
  Auteursrechtelijk beschermd materiaal wordt niet gekopieerd zonder toestemming van de eigenaar. Dit geldt ook voor programmatuur; voor alle aanwezige software (en gebruikers) zijn geldige licenties beschikbaar.

De betrokken verantwoordelijken actualiseren dit beleidsdocument minimaal een keer per 3 jaar of zodra zich belangrijke wijzigingen voordoen.

2.6. Reikwijdte en afbakening

De reikwijdte van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen, voor zowel het gebruik als het beheer daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip, gebruikte systemen en applicaties.
Informatieveiligheid is meer dan alleen de geautomatiseerde informatiesystemen en ICT-infrastructuur. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, beeldscherm enz.) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar vooral ook mensen en processen.

2.7. Grondslagen

Het beleid is gebaseerd op de Strategische en Tactische Baselines Informatiebeveiliging Nederlandse Gemeenten (BIG) versie 1.01. Een nadere uiteenzetting is terug te vinden in hoofdstuk 4 van dit beleidsdocument.

Het gemeente brede Informatieveiligheidsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) veiligheidseisen. Hierbij geldt specifieke wet- en regelgeving waar altijd aan voldaan moet worden, zoals eerder in dit document genoemd. Indien hogere veiligheidseisen worden gesteld vanuit bepaalde kerntaken op grond van wet- en regelgeving dan worden deze eisen geïmplementeerd bovenop de eisen van de BIG.
Dit beleid dekt overigens de AVG niet geheel af. Daarvoor is als basis privacy beleid nodig dat verder gaat in concrete governance, procedures, maatregelen en richtlijnen. Informatieveiligheid heeft uiteraard wel raakvlakken, maar is slechts een van de randvoorwaarden om überhaupt te kunnen voldoen aan de eisen van de AVG.
Bij de uitwerking is het kunnen beschikken (en bijhouden) van een (Informatie)architectuur (blauwdruk van wat je in huis hebt), noodzakelijk om de juiste afwegingen en beslissingen te kunnen maken.

2.8. Risicobenadering

De gemeente volgt een aanpak van Informatieveiligheid op basis van risicobeheersing. Het streven naar 100% veiligheid heeft geen zin, is een utopie en zou te belastend zijn voor de organisatie. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van veiligheidsmaatregelen te implementeren en om daarbij een betere afweging tussen kosten en noodzaak te maken.
Het startpunt voor een gestructureerde opbouw is het uitvoeren van een nulmeting op basis van de BIG en bedoeld om inzicht te krijgen in het zogenaamde ‘gat’ tussen datgene wat nodig is en wat ontbreekt. Op basis van dat inzicht vindt een impactanalyse plaats waardoor de gemeente in staat is om prioritering te geven aan verbeterpunten voor de korte (denk aan ‘Quick Wins’) en lange termijn. Bij deze benadering is ruimte voor afweging en prioritering op basis van het principe ‘pas toe of leg uit’.
Indien een gemeentelijk proces meer beheersingsmaatregelen nodig heeft dan vindt hierop een (uitgebreide) risicoanalyse plaats. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van het werkproces en de dreigingen die kunnen leiden tot een veiligheidsincident.

2.9. Samenwerking

Intergemeentelijke samenwerking en het samenwerken met ketenpartners heeft er al toe geleid dat er steeds vaker en andere informatie wordt uitgewisseld met samenwerkingspartners. De ontwikkelingen in het sociaal domein zijn hiervan een sprekend voorbeeld. Wanneer bij de samenwerking met partners Informatieveiligheid een rol speelt worden afspraken gemaakt over het vereiste niveau van Informatieveiligheid die de gemeente stelt. In sommige gevallen kan dit hoger liggen dan de vereisten volgens de BIG. Denk in dat geval aan privacy gevoelige gegevens.
Een extra dimensie hier is dat er vanaf nu naar wordt gestreefd om het Informatieveiligheidsbeleid van de gemeentes Nieuwegein en Zeist inhoudelijk af te stemmen en synchroon te laten lopen. De gemeentes hebben met de gezamenlijke aanschaf van een nieuwe ICT infrastructuur impliciet de basis gelegd voor onderlinge afstemming van het volgen van de vereisten uit de BIG.

3. Organisatie van de Informatieveiligheid

3.1. Interne organisatie

Om Informatieveiligheid te beheren en blijvend te borgen in de gemeentelijke organisatie is een goed werkend ISMS als denk- en werkwijze nodig waarbij intern duidelijke afspraken zijn gemaakt over de daarbij behorende verantwoordelijkheden, taken en rollen. Het gaat hier over de governance rond Informatieveiligheid waarbij onderlinge samenwerking en afstemming - en ieder vanuit zijn eigen verantwoordelijkheid - bepalend is voor het succes van een goed werkend ISMS.

3.2. Verantwoordelijkheden en rollen

Het college van B&W is bestuurlijk verantwoordelijk voor de veiligheid van informatie binnen de werkprocessen van de gemeente en stelt kaders op voor Informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.
Het college van B&W stelt formeel het Informatieveiligheidsbeleid vast, delegeert de uitvoering hiervan aan het hoofd van de afdeling Informatievoorziening. Het College informeert jaarlijks de raad over dit thema. Binnen het college van B&W valt Informatieveiligheid onder de portefeuille van de bestuurder Informatievoorziening. De CISO adviseert het college van B&W formeel over het vast te stellen beleid.

De Informatiemanager (ook wel Chief Information Officer ofwel CIO genoemd), is het hoofd van de afdeling IV, en is ambtelijk verantwoordelijk voor de veiligheid van informatie en de daarbij behorende algemene sturing. De CIO geeft sturing aan de uitvoering van het beleid met betrekking tot Informatieveiligheid en ziet erop toe dat dit beleid wordt nageleefd. De taken die hieruit voortvloeien zijn belegd bij de Chief Information Security Officer (CISO).

De CISO bevordert en adviseert gevraagd en ongevraagd over Informatieveiligheid en rapporteert jaarlijks concern breed aan het College van B&W over de stand van zaken. De CISO heeft een adviserende, faciliterende en coördinerende rol richting het college van B&W, de directie en lijnmanagement. De directie zorgt ervoor dat uitvoerende taken zoveel mogelijk belegd zijn bij het lijnmanagement. Controlerende taken op het gebied van informatieveiligheid gaan zoveel mogelijk in samenwerking met de afdeling concern control. Een functieprofiel van de CISO is uitgewerkt.
Alle organisatieonderdelen hebben minimaal 1 aanspreekpunt voor de CISO. Periodiek voert de CISO overleg met deze contactpersonen en eventueel andere security gerelateerde medewerkers en voor privacy gerelateerde activiteiten over de stand van zaken en nieuwe ontwikkelingen op het gebied van Informatieveiligheid. De resultaten hiervan neemt de CISO mee in zijn evaluatie.

Het team Informatieveiligheid en privacy, dat aangestuurd wordt door de Chief Information Security Officer (CISO):

- stuurt de organisatie aan op het beheersen van veiligheidsrisico's;
- controleert of de getroffen maatregelen overeenstemmen met de veiligheidseisen en of deze voldoende bescherming bieden;
- neemt daarbij in de overwegingen en maatregelen ook alle privacyaspecten mee;
- adviseert en rapporteert aan bestuur en management gevraagd en ongevraagd op het gebied van informatieveiligheid;
- evalueert periodiek beleidskaders en stelt waar nodig bij.

Het (lijn)management is operationeel verantwoordelijk voor de integrale veiligheid van de organisatieonderdelen. Het lijnmanagement:

- stelt op basis van een expliciete risicoafweging veiligheidseisen vast volgens de classificatie voor zijn informatiesystemen (zie paragraaf 4.2);
- is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit deze eisen;
- stuurt op veiligheidsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en bewustzijn);
- meldt incidenten en rapporteert in hoeverre hun organisatieonderdeel compliant is aan het Informatieveiligheidsbeleid van de gemeente.

en is binnen de functie van de betreffende afdeling verantwoordelijk voor de uitvoering van:
- de veiligheid van de informatievoorziening en implementatie van veiligheidsmaatregelen die voortvloeien uit de veiligheidseisen en bijbehorende risicoanalyses, alsmede privacyaspecten die aan de orde komen;
- alle beheeraspecten van Informatieveiligheid die betrekking hebben op ICT-aangelegenheden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, logging van activiteiten en back-up & recovery;
- maatregelen gericht op veiligheid van personeel zoals screening, geheimhoudingsverklaringen en awareness programma's;
- maatregelen gericht op veiligheid van gebouwen, publieke en werkruimte van de gemeente;
- activiteiten die gericht zijn op het inrichten en beheren van een ISMS.

De gemeente is aangesloten bij de landelijke Informatiebeveiligingsdienst Nederlandse Gemeenten (IBD). Daarbij zijn twee rollen benoemd bij de onderlinge communicatie. De gemeente heeft voor elke rol een medewerker aangewezen alsmede een achtervang daarvoor. Dit zijn de:
- Algemene Contactpersoon Informatiebeveiliging (ACIB)
- Vertrouwde Contactpersoon Informatiebeveiliging (VCIB).

De ACIB is de algemene contactpersoon voor de IBD en heeft de volgende functie:
- Ontvangen van waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten;
- Mogelijkheid om incidenten te melden bij de IBD.

De VCIB is de vertrouwelijke contactpersoon voor de IBD en heeft de volgende functie:
- Ontvangen van waarschuwingen en informatie met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten;
- Mogelijkheid om incidenten, waarbij ook vertrouwelijke gegevens worden uitgewisseld, te melden bij de IBD.

De gemeente kent ook de functie van Technical Information Security Officer (TISO). Deze is verantwoordelijk voor:
- het analyseren en managen van technische risico's;
- het schrijven en managen van technische uitvoeringsrichtlijnen;
- het uitwerken en begeleiden van de te implementeren technische beveiligingsmaatregelen;
- het vertalen van nieuw beleid of wettelijke richtlijnen naar inhoudelijke en passende technische en hierbij behorende procesmatige maatregelen;
- het creëren van draagvlak en bewustwording, rekening houdend met de verschillende belangen in de organisatie.
- het monitoren en managen van technische functies zoals de IDP/IPS (controle op ongeautoriseerde toegang) infrastructuur, firewalls enz.

De TISO rapporteert aan de Informatiemanager.

Maatregelen inzake informatieveiligheid worden bij voorkeur opgesteld en vastgesteld op het organisatorische niveau waar de benodigde kennis en belang van de maatregelen zo optimaal mogelijk kunnen worden belegd. Dit versterkt het verantwoordelijkheidsbesef van betrokkenen en borging van uitvoering en naleving.

3.3. ISMS (Information Security Management System)

De gemeente maakt gebruik van een ISMS bestaande uit een plan-do-check-act cyclus (PDCA-cyclus) om aantoonbaar grip te blijven houden op de diverse voorbereidende, uitvoerende, beherende en controlerende activiteiten die periodiek nodig zijn om informatieveiligheid naar een hoger niveau te tillen. Het inrichten en beheer van een ISMS ligt bij de CISO. Het ISMS ondersteunt de governance van de Informatieveiligheid.

4. Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

4.1. Inleiding

Zoals in paragraaf 2.8 is aangegeven, is het Informatieveiligheidsbeleid van de gemeente gebaseerd op de Strategische en Tactische BIG versie 1.01. Documentatie hierover is standaard beschikbaar via de Informatiebeveiligingsdienst Nederlandse Gemeenten (IBD).
De BIG wordt in januari 2020 opgevolgd door de BIO (Baseline Informatiebeveiliging Overheid, maar hierover meer in hoofdstuk 5). De gemeente is aangesloten op de dienstverlening van de IBD en bij de uitwerking van dit beleid zal zoveel mogelijk gebruik gemaakt worden van reeds beschikbare documentatie en handreikingen van de IBD.
De BIG bestaat uit 2 delen, te weten een strategisch en tactisch deel en is gebaseerd op een internationale standaard en wel de NEN/ISO 27001: 2005 voor het strategische deel en NEN/ISO/27002: 2007 voor het tactische deel.

De Strategische Baseline is feitelijk de 'kapstok' waaraan de elementen van Informatieveiligheid opgehangen worden en is sterk gericht op de governance van Informatieveiligheid. De organisatie en de verantwoording over informatieveiligheid staat hierin centraal.

De Tactische Baseline beschrijft de normen en veiligheidsmaatregelen die een samenhangend stelsel van veiligheidsmaatregelen vormen. Aan de hand van een risicoanalyse wordt bepaald welke maatregelen ingezet worden en in welke mate volgens het principe 'pas toe of leg uit'. Deze maatregelen behoren vervolgens te worden geïmplementeerd en periodiek te worden getoetst op naleving en effectiviteit.
Het implementeren, verdiepen en onderhouden van de baseline binnen de gemeente is een continu leer- en groeiproces. Het is vooral de menselijke factor die hierbij een belangrijke rol speelt en uit dien hoofde is veel aandacht nodig voor het versterken van de bewustwording en acceptatie bij alle medewerkers. Een gemeente kan nog zoveel technische veiligheidsmaatregelen nemen, wanneer medewerkers er niet naar handelen hebben deze maatregelen uiteindelijk aanzienlijk minder effect.
De Tactische Baseline (hierin wordt wel van 'beveiliging' gesproken) hanteert de volgende indeling: Beveiligingsbeleid, Organisatie van Informatieveiligheid, Beheer van bedrijfsmiddelen, Beveiliging van personeel, Fysieke beveiliging, Beheer van communicatie- en bedieningsprocessen, Logische toegangsbeveiliging, Verwerving, ontwikkeling en onderhoud van informatiesystemen, Beheer van incidenten, Bedrijfscontinuïteit en Naleving

De 15 hoofstukken verwijzen naar de indeling uit de tactische BIG. De items beveiligingsbeleid en organisatie van de informatieveiligheid zijn al uitvoerig behandeld in dit beleidsdocument. In de volgende paragrafen wordt nader ingegaan op de overige thema's.

4.2. Beheer van de bedrijfsmiddelen

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen en dienen te worden beschermd. Deze middelen kunnen immers blootgesteld zijn aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik. Van belang is dat alle relevante bedrijfsmiddelen bekend zijn, voorzien zijn van een eigenaar/hoofdgebruiker en voorzien zijn van geschikte veiligheidsmaatregelen. De procedures configuratiebeheer, dataclassificatie en de baselinetoets ondersteunen de organisatie om grip te houden op het beheer van bedrijfsmiddelen.
Informatie kan meer of minder gevoelig of kritisch zijn en voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Voor dataclassificatie is de volgende tabel in het kader van de BIG van toepassing:

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: gemeentelijke informatie op de website)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

Het gemarkeerde deel is afgedekt door de BIG. Voor kritische informatie die daarbuiten valt, zijn aanvullende veiligheids- dan wel privacy maatregelen nodig. Deze komen in beeld aan de hand van een gedegen risicoanalyse. Het streven is om een zo passend mogelijk classificatieniveau te bepalen. Het object van classificatie is informatie en classificatie vindt plaats op het niveau van werkprocessen en bijbehorende informatiesystemen. De eigenaar van de gegevens bepaalt het niveau van classificatie en houdt daarbij eveneens rekening met wettelijke eisen.

4.3. Veiligheid van inzet van personeel

De veiligheid van inzet van personeel is een van de belangrijkste aandachtsgebieden vanwege het gegeven dat de meeste veiligheidsincidenten te maken hebben met ongewenst menselijk handelen (fouten, diefstal, fraude of misbruik van voorzieningen). Het gaat dan zowel om eigen en ingehuurd personeel als externe gebruikers. Bij de veiligheid van inzet van personeel is onderscheid in een drietal deelgebieden, te weten (1) voorafgaand aan het dienstverband, (2) tijdens het dienstverband en (3) bij beëindiging of wijziging van het dienstverband.
Bij ‘voorafgaand aan het dienstverband’ gaat het er om te bewerkstelligen dat de betrokkenen hun verantwoordelijkheden begrijpen en te toetsen of ze geschikt zijn voor de overwogen rollen om daarmee het risico op diefstal, fraude of misbruik van faciliteiten te verminderen
Tijdens het dienstverband ligt de nadruk op het bewerkstelligen dat betrokkenen zich bewust zijn van bedreigingen en gevaren voor Informatieveiligheid, hun verantwoordelijkheden en de zaken waarvoor zij aansprakelijk gesteld kunnen worden. Bovendien gaat het er om dat zij zijn toegerust om het veiligheidsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico op een menselijke fout te verminderen.
Bij beëindiging of wijziging van het dienstverband gaat het er om te bewerkstelligen dat betrokkenen de organisatie ordelijk verlaten dan wel dat wijziging van het dienstverband ordelijk verloopt.

4.4. Fysieke veiligheid

Fysieke veiligheid is gericht op het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
Aandachtsgebieden zijn de fysieke toegang tot gebouwen, publieke ruimten en werkruimten, maar ook het fysiek afschermen van ICT-voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen (bekabeling, werkstations, computerruimte, etc.). Je kunt hierbij denken aan maatregelen zoals ‘hardening’, ‘pentesten’ en two-factor tenzij.

4.5. Beheer van communicatie- en bedieningsprocessen

Het beheer van communicatie- en bedieningsprocessen is gericht op het handhaven van de noodzakelijke veiligheidseisen die gesteld zijn aan het beheer en gebruik van ICT-voorzieningen binnen de gemeente.
Aandachtsgebieden zijn de borging van de integriteit van de ICT-voorzieningen, programmatuur en infrastructuur zowel intern (ICT-afdeling) als extern (bij uitbesteding en samenwerkingsverbanden) om zoveel mogelijk fouten, storingen, uitval en problemen rondom de continuïteit van de (digitale) dienstverlening te voorkomen dan wel te kunnen herstellen.

4.6. Logische toegangsveiligheid

Logische toegangsveiligheid is het geheel aan maatregelen met als doel de toegang tot gegevens en informatiesystemen te beheersen, zodat gegevens, informatiesystemen en apparatuur worden beschermd tegen ongeautoriseerde handelingen.
Aandachtsgebieden zijn het definiëren en beheren van toegangsbeleid, -voorzieningen en -rechten van gebruikers waarin is aangegeven aan welke bedrijfseisen de toegangsveiligheid moet voldoen en waarbij rekening gehouden wordt met afzonderlijke bedrijfstoepassingen zowel intern als toegang via externe werkplekken (thuiswerkplek) en via mobiele apparatuur en waarbij de eigen verantwoordelijkheid van gebruikers nadrukkelijk aan de orde is. Dus onder andere het toepassen van Role based acces (RBA), als verplichting vanuit de verschillende normen en de AVG.

4.7. Verwerving, ontwikkeling en onderhoud van informatiesystemen

Dit onderdeel gaat vooral in op de veiligheid van informatiesystemen en het onderhoud op deze informatiesystemen. Informatiesystemen omvatten besturingssystemen, infrastructuur, bedrijfstoepassingen en toepassingen die ten dienste staan van de (digitale) dienstverlening.
Aandachtsgebieden zijn het organiseren van Informatieveiligheid bij inkoop, acceptatie, bescherming, beheer en wijzigingen bij aanschaf van nieuwe informatiesystemen of onderdelen ervan alsmede de informatie daarin.

4.8. Beheer incidenten Informatieveiligheid

Het beheer van incidenten aangaande Informatieveiligheid is een belangrijk aandachtsgebied in het kader van Informatieveiligheid en dit belang is alleen maar toegenomen vanwege de meldplicht datalekken vanaf 2016 en de invoering van de AVG in 2018. Een veiligheidsincident kan leiden tot ernstige reputatieschade en extra kosten als gevolg van herstelmaatregelen. Het voorkomen of minimaliseren van incidenten is uiteraard beter zoals het implementeren van de preventieve maatregelen uit de tactische BIG, echter incidenten zijn niet uit te bannen en dus zal de organisatie hierop voorbereid moeten zijn.
Aandachtgebieden zijn het snel en adequaat te kunnen reageren op veiligheidsincidenten en datalekken en daar lering uit trekken. Van belang is hier dat alle medewerkers is in staat zijn veiligheidsincidenten en datalekken te herkennen en weten hoe zij deze incidenten moeten melden.

4.9. Continuïteitsbeheer

Bij continuïteitsbeheer gaat het om maatregelen die gericht zijn om langdurige onderbreking van bedrijfsactiviteiten bij de gemeente tegen te gaan en om kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen. Het gaat hier niet alleen om de BRP en BAG, waar continuïteitsbeheer een verplicht onderdeel is, maar om een gemeente brede aanpak.
Continuïteitsplannen waaronder uitwijkmogelijkheden en het periodiek testen en evalueren van deze plannen spelen hierbij een belangrijke rol. Het gaat hierbij niet enkel om de ICT voorzieningen, maar ook om de plannen en voorzieningen om, bij een catastrofe die de gemeentelijke gebouwen aangaat, de dienstverlening elders te kunnen voortzetten.

4.10. Naleving

In dit onderdeel ligt de nadruk op het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen. Er zijn vele wetten en regelgeving van toepassing op de gemeente zoals eerder genoemd in dit document.
Een ander belangrijk punt is dat de gemeente moet voldoen aan de gestelde licentie-eisen op programmatuur om eventuele toekomstige boetes/claims van leveranciers te voorkomen.

5. Baseline Informatieveiligheid Overheid

5.1. Baseline Informatieveiligheid Overheid (BIO)

De BIG (Baseline Informatieveiligheid Gemeenten) is het normenkader voor de beveiliging van informatiesystemen (zie hoofdstuk 4). Deze norm wordt per 1 januari 2020 opgevolgd door de Baseline Informatieveiligheid Overheid (BIO). Dan gaan Gemeenten, Rijk, waterschappen en provincies over op één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO), met daarin alle regels waaraan alle overheidslagen moeten voldoen. Voor gemeenten is 2019 voorzien als voorbereidingsjaar. [2]

Informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een vernetwerkte overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners.
De BIO betekent een verandering voor gemeenten. Ten opzichte van de huidige Baseline Informatieveiligheid Gemeenten (BIG) worden bijna 200 maatregelen geschrapt. Gemeenten krijgen zo meer ruimte om voor hen relevante maatregelen te treffen. De maatregelen uit de BIG die in de BIO nog wel worden genoemd gelden als verplicht voor alle overheden.

De BIO positioneert de bestuurder en het management sterker dan voorheen in de rol waarin hij of zij risico-gebaseerd stuurt op het gebied van informatieveiligheid. Zij zullen hierover met de betrokken Chief Information Security Officers afspraken moeten maken. Ter ondersteuning daarbij zijn ‘De 10 bestuurlijke principes voor informatiebeveiliging’ vastgesteld. Ze dienen als handvatten voor dat gesprek. Overigens hanteert Zeist risicomanagement in de afgelopen jaren al als uitgangspunt bij het vormgeven van Informatieveiligheid.

Met de BIO wordt informatiebeveiliging nog meer dan voorheen een zaak van de bestuurder. De BIO positioneert de bestuurder en het management sterker dan voorheen in de rol waarvan hij/zij risico gebaseerd stuurt op het gebied van Informatieveiligheid. Daarnaast is het cruciaal in de BIO dat de verantwoordelijkheid voor informatiebeveiliging wordt belegd bij de lijnmanagers (afdelingshoofden). Ter ondersteuning zijn 10 bestuurlijke principes voor informatieveiligheid vastgesteld.

5.2 De bestuurlijke principes

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid hebben om de gegevens van hun inwoners onder alle omstandigheden te beschermen.

De risico’s rondom de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) maken dat het onderwerp informatiebeveiliging niet mag ontbreken op de bestuurstafel.

[2] https://vng.nl/files/vng/brieven/2019/20190107_ledenbrief_standaardverklaring-baseline-informatiebeveiliging-overheid.pdf

Binnen informatieveiligheid is ICT slechts een onderdeel, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt.

In aanvulling op eerder genoemde baseline (BIO) zijn door de VNG de bijbehorende principes voor bestuurders vastgesteld [3]. Dit document is de bestuurlijke aanvulling op de baseline en helpt de bestuurder om de juiste dingen te doen. De principes gaan vooral over de rol van het bestuur bij het (verder) borgen van informatiebeveiliging in de organisatie. Daarmee gaat dit document over waarden die u zichzelf als bestuurder oplegt dienen daarom verbonden te zijn aan de waarden van de organisatie. De 10 bestuurlijke principes zijn:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Zoals eerder aangegeven is naast het nog meer betrekken van de bestuurder in de informatiebeveiliging ook een belangrijke rol weggelegd voor de lijnmanagers. Daar zit een uitdaging. De verantwoordelijkheid voor de informatieveiligheid komt meer dan voorheen te liggen bij die lijnmanager. Die zal vaker dan voorheen zelf beslissingen moeten nemen. Een en ander heeft (of kan) ook gevolgen hebben voor de verhouding tussen de lijnmanager (veelal de proceseigenaar) en de CISO (Chief Information Security Officer).

Een belangrijke taak is de komende jaren dan ook om, met behulp van de BIO, de lijnmanager te overtuigen van nut en noodzaak van informatiebeveiliging en te helpen bij het inrichten daarvan. Dat kan door het uitvoeren van risicomanagement, ten behoeve en op basis van het bedrijfsbelang van het proces. Het is hierbij belangrijk dat ieder bedrijfsmiddel een eigenaar heeft. Dat geldt ook voor processen, hardware en software, want als er niemand van is worden er mogelijk ook geen passende maatregelen genomen om deze adequaat te beschermen. Iedere computer en ieder softwarepakket heeft zijn zwakheden en als je niet weet welk apparaat of pakket je in huis hebt, kun je op voorhand ook niet de juiste maatregelen nemen ze te beschermen.

[3] *'De 10 bestuurlijke principes voor informatiebeveiliging'.* *https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf*

6. Eenduidige Normatiek Single Information Audit (ENSIA)

Vanaf 2017 is er een landelijk kader voor alle Nederlandse gemeentes om rekenschap te kunnen geven over het gevoerde beleid inzake Informatieveiligheid.
De *Eenduidige Normatiek Single Information Aud*it (ENSIA) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeentes verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken, de Vereniging van Nederlandse Gemeenten (VNG), gemeentes, het ministerie van Sociale Zaken & Werkgelegenheid en het ministerie van Infrastructuur & Milieu.
Met de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” van 2013 hebben alle gemeentes afgesproken de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) te implementeren. Deze baseline is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.
Uitgangspunt van ENSIA is *de single information audit*. Dit betekent dat de gemeente maar één keer per jaar de zelfevaluatielijst hoeft in te vullen. De informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad. Het gaat hier enerzijds om een jaarlijkse horizontale verantwoording via het college van B&W en gemeenteraad via een zelfevaluatie van de Tactische BIG, waarbij op basis van risicoschattingen en prioritering inzicht wordt gegeven van welke BIG maateregelen al of niet – ‘leg uit of pas toe’ – ingevoerd zijn. Anderzijds is er een jaarlijkse verticale verantwoording richting de centrale overheid voor het veilig inrichten en gebruik van:

de basisregistraties:

- Basisregistratie Adressen en Gebouwen — BAG (belegd bij Geo)
- Basisregistratie Grootschalige Topografie — BGT (belegd bij Geo)
- Basisregistratie Ondergrond — BRO (vanaf 2019)
- Basisregistratie Personen — BRP (belegd bij Burgerzaken)
- Paspoortuitvoeringsregeling Nederland 2001 — PUN (belegd bij Burgerzaken)

en centrale voorzieningen:

- Digitale Identiteit — DigiD (e-loket gemeente)
- Suwinet — Inkijk (Burgerzaken, RMC en Regionale Sociale Recherche)

Voor alle hierboven genoemde administraties en voorzieningen wordt een gerichte zelfevaluatie uitgevoerd door de gemeente, gebaseerd op een voor iedere toepassing toegespitst normenkader. De laatst genoemde twee zelfevaluaties worden daarna ook geaudit door een externe auditor. De auditverslagen worden dan goedgekeurd door het college B&W.
Het geheel van zelfevaluaties wordt dan gerapporteerd/verantwoord met de eventuele auditverslagen richting de betrokken ministeries.

Inzake de hierboven genoemde voorzieningen moet ook het volgende opgemerkt worden:

- Bij de DigiD aansluiting is er een verplichting om op alle normen voldoende te scoren, op straffe van het afsluiten van de DigiD aansluiting bij onvoldoende prestatie.
- Bij Suwinet wordt geaudit op een subset van de voor Suwinet gestelde normen, waarbij het van belang is dat de gemeente gedocumenteerd aan kan tonen hoe het aansluitbeleid op Suwinet is georganiseerd en geborgd. De gemeente heeft hiervoor een apart beheer document dat op afdelingsniveau wordt beheerd en vastgesteld.
- Bij de BRP is op grond van bepalingen binnen de Wet basisregistratie personen (Wet BRP) het college van B&W verplicht om vastgestelde regels omtrent de technische en

administratieve inrichting, de werking en de beveiliging van de Basisregistratie Personen na te leven. In relatie tot het onderzoek dient het Informatiebeveiligingsbeleid Basisregistratie personen, op grond van artikel 11 van de Wet basisregistratie personen, operationeel te zijn. De gemeente heeft hiervoor een apart beheer document dat op afdelingsniveau wordt beheerd en vastgesteld.

- Bij de Paspoort Uitvoeringsregeling Nederland 2001 (PUN-2001) op grond van artikel 93 en op grond van artikel 128, lid 1 van het Reglement rijbewijzen, is de burgemeester verplicht te voorzien in een op schrift gestelde beveiligingsprocedure. Het onderhavige document wordt geacht daarvan het directe gevolg te zijn. Met de vaststelling van deze beleidsnotitie worden tevens alle in het Informatiebeveiligingshandboek opgenomen procedures bekrachtigd als beveiligingsprocedure. De gemeente heeft hiervoor een apart beheer document dat op afdelingsniveau wordt beheerd en vastgesteld.

Met ENSIA is er hiermee voor de gemeente een gestructureerd en verplicht handvat en richtlijn om zowel het principe van verbetering van de Informatieveiligheid (Plan-Do-Check-Act) op bestuurlijk niveau (B&W en raad) als ook de verwerking ervan met behulp van een ISMS formeel te regelen en is de cirkel rond.

7. Algemene Verordening Gegevensbescherming (AVG)

Op 21 oktober 2013 is de Algemene Verordening Gegevensbescherming (AVG) aangeboden aan het Europese parlement. Nadat deze op 25 mei 2016 in werking is getreden, hebben nationale overheden bedrijven en overheidsinstanties 2 jaar de tijd gegeven om aan de bepalingen van de AVG te voldoen. In de AVG is verder uitwerking gegeven aan het grondrecht van eerbiediging van de persoonlijke levenssfeer. Het toezicht op de naleving van deze wet ligt bij de Autoriteit Persoonsgegevens. Door recente wetswijzigingen heeft de Autoriteit aan kracht gewonnen. Zo zijn de maximale boetebedragen die de Autoriteit kan opleggen sterk verhoogd en zijn organisaties die persoonsgegevens verwerken verplicht om datalekken te melden.
Inmiddels is bescherming van persoonsgegevens (Wet bescherming persoonsgegevens ofwel de Wbp) naar Europees niveau getild (General Data Protection Regulation ofwel GDPR). Op 25 mei 2016 is de AVG in werking getreden en moeten verwerkingsverantwoordelijken (waaronder gemeenten) vanaf 25 mei 2018 aan de Verordening voldoen. De Wet bescherming persoonsgegevens zal deels worden overgeheveld naar de Uitvoeringswet Algemene Verordening Gegevensbescherming en voor het overige worden ingetrokken.

De gemeente stelt een apart privacy beleid op dat wordt vastgesteld door B&W. Dit privacy beleid wordt gelijk met het onderliggende Informatieveiligheidsbeleid 2018 aan het College aangeboden. Over het privacy beleid heeft afstemming plaatsgevonden met de overige vier gemeenten, te weten De Bilt, Bunnik, Utrechtse Heuvelrug en Wijk Bij Duurstede. Voor deze vijf gemeentes is in 2018 vanuit de AVG een gezamenlijke Functionaris voor de Gegevensbescherming (FG) aangesteld. Informatieveiligheid en privacy zijn nauw verbonden met elkaar. De FG werkt dan ook nauw samen met de CISO op dit gebied.

8. Begrippenlijst

- Informatieveiligheid: samenhangend stelsel van beheersingsmaatregelen dat de beschikbaarheid / continuïteit, de integriteit / betrouwbaarheid en vertrouwelijkheid / exclusiviteit van de informatie garandeert (BIV).
- Beschikbaarheid / continuïteit: zorgen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit / betrouwbaarheid: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid / exclusiviteit: beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

CIO	Chief Information Officer
CISO:	Chief Information Security Officer
TISO:	Technical Information Security Officer (TISO)
PO:	Privacy Officer
PJ:	Privacy Jurist
FG:	Functionaris voor de Gegevensbescherming: FG
AVG:	Algemene Verordening gegevensbescherming
GDPR:	General Data Protection Regulation: GDPR
WBP:	Wet Bescherming persoonsgegevens
IBD:	Informatiebeveiligingsdienst Nederlandse Gemeenten (IBD).
ACIB:	Algemene Contactpersoon Informatiebeveiliging
VCIB:	Vertrouwde Contactpersoon Informatiebeveiliging.
ISMS:	Information Security Management System
ENSIA:	Eenduidige Normatiek Single Information Audit
BIG:	Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
BIO:	Baseline Informatieveiligheid Overheid)
Suwinet:	Digitale infrastructuur voor uitwisseling tussen suwipartijen van gegevens
BAG:	Basisregistratie Adressen en Gebouwen
BGR:	Basisregistratie Grootschalige Topografie
BRO:	Basisregistratie Ondergrond BRO
BRP:	Basisregistratie Personen BRP
PUN2001:	Paspoortuitvoeringsregeling Nederland 2001
DigiD:	Digitale Identiteit
RBA:	Role based acces
PDCA cyclus:	Plan-Do-Check-Act cyclus