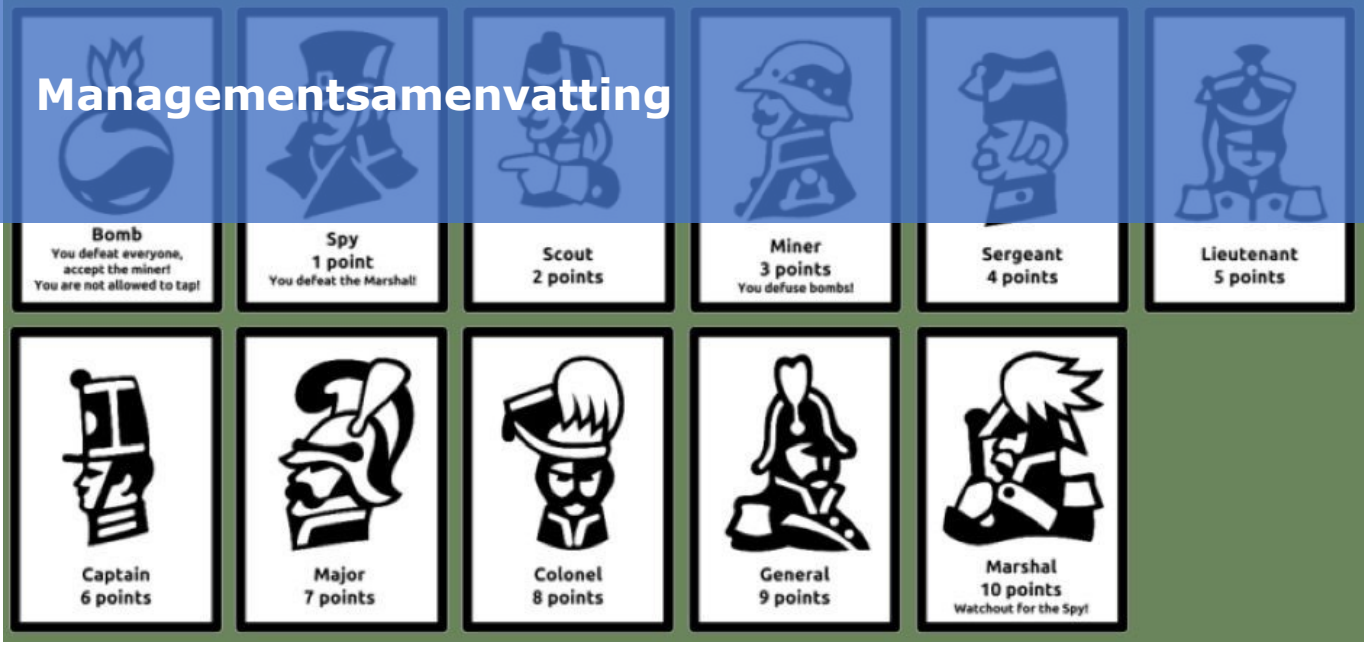
Managementsamenvatting



Informatie is een uiterst belangrijk bedrijfsmiddel van de gemeente Velsen. Van hoog tot laag, van maarschalk tot verkenner in Stratego-termen, is iedere medewerker afhankelijk van informatie voor de, te verrichten, taken. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente als dienstverlener en de basis voor het beschermen van rechten van burgers en bedrijven.

Het beleid is strategisch en beschrijft vooral de ambitie en visie en de voorwaarden en uitgangspunten die nodig zijn om die te realiseren. Het vormt de basis voor tactische beleidsuitwerkingen op deelgebieden.

Met dit beleid dragen we bij aan het vergroten van de betrouwbaarheid van de informatievoorziening. Dit valt uiteen in drie begrippen: beschikbaarheid, integriteit en vertrouwelijkheid. Informatiebeveiliging is het proces dat er voor zorgt dat de betrouwbaarheid voldoende (d.w.z.: op het afgesproken niveau) is. Door periodieke controle, organisatie-brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening voor de hele organisatie benaderd. Het plan wordt jaarlijks opnieuw opgesteld op grond van de stand van zaken m.b.t. naleving van de BIO, ontwikkelingen, controles en registraties in het incidentenregister. Hoe de beveiliging van informatie wordt ingericht is voor een groot deel afhankelijk van de dreigingen. De grootste bedreiging is anno 2023 een vorm van cybercriminaliteit, bekend onder de naam Ransomware. De informatiebeveiligingsdienst heeft een, speciaal op digitale weerbaarheid gericht, maatregelenpakket samengesteld die aan die dreiging het hoofd biedt. De focus zal in de komende tijd liggen op het compleet in werking krijgen van deze maatregelen.

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico’s die de gemeente hiermee loopt en welke van deze risico’s onacceptabel hoog zijn.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligings-beleid van en voor de hele gemeente. Daarvoor hanteert het management een aantal uitgangspunten over het belang van de informatievoorziening, verantwoordelijkheden,

verankering van informatiebeveiliging in de organisatie, continu verbeteren en het beschikbaar stellen van mensen en middelen.

Informatiebeveiliging raakt alle onderdelen van de organisatie. Het is daarom nodig verantwoordelijkheden, rollen, taken en bevoegdheden volstrekt helder te hebben en daarom lichten we ze hieronder toe.

- Het college van Burgemeester en Wethouders is integraal eindverantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Als zodanig stelt het college informatiebeveiligingsbeleid vast, delegeert de uitvoering aan de directie en informeert de gemeenteraad over dit thema.
- De Directie is verantwoordelijk voor de beveiliging van informatie en bijbehorende aansturing van het lijnmanagement. Zij wordt daarin met adviezen en coördinatie ondersteund door de Chief Information Security Officer (CISO).
- Het lijnmanagement van de gemeente is verantwoordelijk voor de integrale beveiliging van de organisatieonderdelen, eveneens ondersteund door de CISO. De lijnmanager zorgt voor het beleggen van taken met betrekking tot beveiliging bij de juiste medewerkers en stimuleert al zijn of haar medewerkers tot het vertonen van een veilige werkwijze.

Het college van Burgemeester en Wethouders legt verantwoording af over informatiebeveiliging en hanteert daarvoor de ENSIA[1]-systematiek. Met deze systematiek wordt enerzijds de gemeenteraad op de hoogte gesteld van de stand van zaken en anderzijds de ministeries die namens het Rijk toezicht houden op het gebruik en de kwaliteit van delen van de informatievoorziening. De CISO treedt hierbij op als coördinator. Nieuwe Europese wetgeving, de netwerk en informatiebeveiligingsrichtlijn (NIB2), vertaald in de nationale wet beveiliging netwerk en informatiesystemen (wbni) heeft waarschijnlijk vergaande consequenties voor de decentrale overheid. Er is hierover nog onduidelijkheid maar de kans is groot dat deze wordt aangemerkt als essentiële entiteit. Daarmee kan dan het toezicht door de Rijksoverheid strenger worden. Gemeentes zullen de naleving van de BIO volledig moeten aantonen zoals dat bij een certificering volgens de ISO27001 ook het geval is.

Basis voor de inrichting van een goed systeem om informatiebeveiliging te beheersen wordt de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft in 14 hoofdstukken alle aspecten om de informatievoorziening voldoende te beveiligen en is gebaseerd op de internationale standaarden ISO27001 en ISO27002.
De BIO geeft de organisatie de mogelijkheid om voor bedrijfsprocessen/informatiesystemen beveiligingsniveaus vast te stellen. De manager bepaalt, door middel van een risicoafweging, welk beveiligingsniveau passend is bij het deel van de informatievoorziening waar hij of zij verantwoording voor draagt. Uit het niveau volgt vervolgens welke beheersmaatregelen daarbij opgevolgd dienen te worden.

De risicoafweging om het beveiligingsniveau te bepalen zal in eerste instantie voor de kritieke processen worden uitgevoerd. Daarna zullen andere (hoofd)bedrijfsprocessen onder de loep genomen worden. Het gaat om de volgende kritieke processen:

- Beheer basisregistraties
- Belastingheffing en inning
- Dienstverlening Burgerzaken
- Dienstverlening Sociaal Domein
- Financiële administratie
- Bedrijfsprocessen openbare orde en veiligheid
- Vergunningverlening
- Beheer personeelszaken

[1] *Eénduidige Normatiek Single Information Audit*

1. Inleiding

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente Velsen. Immers, de gemeente is in de kern een informatiehuishouding, beheert veel persoons- en privacygevoelige gegevens en behoort daarom veilig en zorgvuldig om te gaan met informatie en het uitwisselen van informatie.

Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van informatie kan leiden tot ernstige gevolgen voor (de continuïteit van) de bedrijfsvoering, en tot imagoschade met mogelijk politieke gevolgen. En er kunnen gevolgen zijn voor individuele personen als gegevens over hen worden gestolen. Zij kunnen dan makkelijker benaderd worden door criminelen voor bijvoorbeeld oplichterspraktijken of hun identiteit kan worden misbruikt voor frauduleuze handelingen. Met het laatste kunnen onschuldige personen in verband gebracht worden met criminaliteit en daar enorm veel problemen mee krijgen.

De almaar toenemende digitalisering brengt "nieuwe" bedreigingen met zich mee waarvan criminele activiteiten op internet een belangrijk deel uitmaken. De samenleving is daar in de afgelopen jaren diverse malen door getroffen. De grootste bedreiging anno 2023 is Ransomware[2]. Deze vorm van afpersing heeft veel bedrijven getroffen en ook gemeenten worden er in toenemende mate slachtoffer van. Er zijn veel maatregelen en grote waakzaamheid nodig om weerbaar te zijn. De informatiebeveiligingsdienst heeft specifieke maatregelen in beeld gebracht die de digitale weerbaarheid verhogen.

Om de gemeenten in staat te stellen op een efficiënte manier verantwoording af te leggen over informatiebeveiliging is de systematiek ontwikkeld die bekend staat als ENSIA[3]. Deze is in 2017 gelanceerd en bestaat uit een zelfevaluatie waarmee in één keer jaarlijks verantwoording wordt afgelegd aan de gemeenteraden én aan de ministeries die verantwoordelijkheid dragen voor specifieke deelgebieden (BRP, PUN, BAG, BGT, DigiD en Suwinet). Daarmee zijn de verschillende aparte audits komen te vervallen. Daarentegen gaat deze zelfevaluatie over informatiebeveiliging in brede zin en is daardoor veelomvattender. Het vergt dan ook een behoorlijke inspanning om alle informatie bij elkaar te krijgen waarmee de vragen beantwoord kunnen worden.

Met de komst van de Europese Algemene Verordening Gegevensbescherming (AVG) in 2018 is privacy in het brandpunt van de belangstelling komen te staan. Gemeenten zijn druk doende om aan deze wetgeving te kunnen voldoen. Informatiebeveiliging is een

[2] Ransomware is een vorm van kwaadaardige software die er voor zorgt dat alle bestanden in een ICT-systeem versleuteld en onleesbaar worden. Criminelen eisen vervolgens losgeld om de versleuteling ongedaan te maken. Om de afpersing kracht bij te zetten worden (persoons)gegevens gestolen en gepubliceerd in criminele kanalen.
[3] ENSIA is de afkorting van Eénduidige Normatiek Single Information Audit.

belangrijke voorwaarde om een zorgvuldige omgang met persoonsgegevens te kunnen garanderen.

De gemeente Velsen kan het zich dus niet veroorloven om op dit onderwerp achterover te gaan leunen. De ontwikkelingen gaan snel en het is zaak om bij te blijven en de juiste maatregelen in werking te hebben om risico's te beheersen.

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot 2027.
De nota is richtinggevend en stelt kaders. Daar waar dit vereist is of nodig wordt geacht op basis van risicomanagement, worden door de gemeente aanvullende tactische beleidsdocumenten opgesteld. Dit zijn onderwerpen als wachtwoordbeleid, beleid voor toegang tot ICT-systemen, back-up en fysieke toegang tot de bedrijfsgebouwen. Op operationeel niveau wordt het beleid vertaald in ICT-procedures, zoals voor het oplossen van incidenten, doorvoeren van wijzigingen in hard- en software en in stand houden van een noodvoorziening met reservekopieën (back-up). Naleving van deze documenten is de verantwoordelijkheid van de lijnmanager. Deze wordt daarbij ondersteund met coördinerende en controlerende activiteiten door de CISO en Concern Control.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2023-2027' continueert de gemeente Velsen de beveiliging van persoonsgegevens en andere informatie en bouwt voort op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)[4]. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG[5].

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp-specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. Dit zijn onderwerpen als informatie-uitwisseling, beveiliging van mobiele apparatuur, logische toegangsbeveiliging en fysieke toegangsbeveiliging. In het jaarplan informatiebeveiliging (opgesteld door de CISO, vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van leidinggevenden, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. ENSIA dient daarbij als meting om te bepalen in hoeverre er invulling wordt gegeven aan het beleid. In het plan staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is vastgelegd. De acties worden ingepland en, met behulp van het beheersysteem voor informatiebeveiliging, toebedeeld aan medewerkers die ze moeten uitvoeren.
Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.
Hoofdstuk 4 geeft een beschrijving in hoofdlijnen van de BIO en hoe deze als kader voor risicomanagement gehanteerd dient te worden.

1.2 Mandaat

Vast stellen van het strategisch beleid is voorbehouden aan het College van Burgemeester en Wethouders. Het college geeft de directie het mandaat om beleid op tactisch niveau vast te stellen.

[4] Zie bijlage C.
[5] Zie bijlage B.

1.3 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juist, volledig en actueel) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.4 Ambitie en visie van de gemeente Velsen

In de afgelopen jaren is gebleken dat de implementatie van informatiebeveiliging volgens de Baseline Informatiebeveiliging Overheid geen sinecure is. Anno 2023 heeft de gemeente Velsen nog niet alle maatregelen in werking om geheel aan de norm te voldoen.
De komende jaren zet de gemeente Velsen daarom in op het tot stand brengen van alle noodzakelijke verbeteringen en zorgt er voor dat de beveiligingsmaatregelen blijven werken. De gemeente houdt focus op de professionalisering van de informatiebeveiligingsfunctie in de organisatie.
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente als dienstverlener en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Uit de jaarlijkse ENSIA-verantwoording blijkt dat gemeente Velsen in 2023 nog niet aan alle beveiligingsnormen voldoet. Om onnodige risico's te vermijden dienen de ontbrekende maatregelen ingevoerd te worden, tenzij ze niet van toepassing zijn. Daarnaast is het nodig om de getroffen maatregelen te blijven toetsen op hun werking zodat deze tijdig verbeterd worden. Gezien de grote dreiging van Ransomware is het belangrijk om de maatregelen voor het verhogen van digitale weerbaarheid in werking te hebben. Gemeente Velsen heeft dat al voor een groot deel voor elkaar maar er ontbreken nog een paar belangrijke bouwstenen. In de komende tijd zal de focus op deze maatregelen liggen.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een schepper van mogelijkheden; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals tijds- en plaats-onafhankelijk werken. De focus is 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. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2023 tot 2027'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarplan informatiebeveiliging. Dit jaarplan komt tot stand in een continue cyclus van verbetering, ook wel de Plan, Do, Check, Act-cyclus (PDCA-cyclus) genoemd. Het samenspel van beleid, planning en Beheersmaatregelen is het Information Security Management System (ISMS).

2.2 Kader

Een divers scala aan wet en regelgeving is van belang voor de actualisering van het informatiebeveiligingsbeleid. Maar met name de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) zijn van invloed. In 2013 heeft de VNG besloten om de beveiliging van informatievoorzieningen te baseren op de Baseline Informatiebeveiliging Gemeenten. Die is in 2019 vervangen door de BIO.

2.2.1 De Baseline Informatiebeveiliging Overheid

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat leidinggevenden moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes over beveiligingsniveau's voor informatiesystemen maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. In hoofdstuk 4 wordt nader op de BIO ingegaan.

2.2.2 Wet beveiliging netwerk- en informatiesystemen (WBNI)

De WBNI vertaalt de Europese Network and Information Security directive (NIS2/NIB2) naar Nederlandse wetgeving. De NIB2 is een herziening van de, eveneens Europese NIB en beoogt een goede samenwerking tussen de lidstaten op het gebied van cybersecurity. De NIB-richtlijn bevat beveiligingsverplichtingen voor aanbieders van digitale diensten. De NIB2 breidt het toepassingsgebied van de bestaande NIB-richtlijn uit naar diverse sectoren die belangrijk zijn voor de economie en samenleving. Ongeveer 4000 instellingen, waaronder het openbaar bestuur, worden verplicht om meer maatregelen te nemen om cyberbeveiligingsrisico's te beheersen. Zo moeten ze aan strengere beveiligings- en rapportagevereisten voldoen.

Daarnaast wordt in de NIB2 bepaald dat de nationale autoriteiten strenger moeten handhaven op het naleven van de regels. Er zal sprake zijn van een proactief beleid waarbij controles steekproefsgewijs worden uitgevoerd. Het doel van deze richtlijn is dus meer dan ooit om cybersecurity op een fatsoenlijk niveau te brengen en houden. Wanneer bedrijven en entiteiten hun beveiligingseisen niet op orde hebben zal dit waarschijnlijk vaker resulteren in meer en hogere boetes. De boetes kunnen oplopen tot ten minste 10 miljoen euro of 2% van de totale wereldwijde omzet.

Publieke organisaties vallen onder de nieuwe richtlijn maar er is nog veel onduidelijk. Momenteel lijkt het erop dat het ministerie van Justitie en Veiligheid voornemens is om decentrale overheden aan te merken als essentiële entiteit in de WBNI.
De wet kan dan vergaande consequenties hebben voor de gemeenten. Naast een meldplicht voor informatiebeveiligingsincidenten met grote impact kan ook het toezichtregime (veel) strenger worden dan nu en zou het kunnen dat gemeentes de naleving van de BIO volledig aantoonbaar moeten maken zoals in het bedrijfsleven bij een ISO27001-certificering. Daarbij is het nodig om te sturen op risicomanagement.

2.2.3 Algemene Verordening Gegevensbescherming

De Europese Algemene Verordening Gegevensbescherming is mei 2018 van kracht geworden. Deze wet heeft een directe werking en is voor alle EU-lidstaten gelijk. In Nederland is daardoor de Wet Bescherming Persoonsgegevens komen te vervallen. Met de AVG zijn de regels rondom privacy aangescherpt. De belangrijkste wijzigingen zijn:

- de verplichting om een actueel register van verwerkingen van persoonsgegevens te hebben,
- de meldplicht datalekken[6],
- de toegenomen bevoegdheden van de toezichthouder privacy[7], waaronder het opleggen van zeer hoge boetes.

Naast deze wet zijn er nog diverse andere wetten van belang voor informatiebeveiliging. De belangrijkste voor de gemeentelijke praktijk zijn:

- wet structuur uitvoeringsorganisatie werk en inkomen (SUWI),
- paspoortwet,
- wet basisregistratie personen (BRP),
- wet basisregistratie Adressen en Gebouwen (BAG),
- wet basisregistratie Grootschalige Topografie (BGT),
- wet basisregistratie Ondergrond,
- Archiefwet.

2.2.4 De 10 principes voor informatiebeveiliging

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 informatiebeveiliging. Zij zullen hierover met de betrokken Chief Information Security Officer afspraken moeten maken. Ter ondersteuning daarbij zijn 'De 10 bestuurlijke principes voor informatiebeveiliging'[8] vastgesteld. De 10 principes voor informatiebeveiliging zijn aldus een bestuurlijke aanvulling op het normenkader [9] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt geformuleerd:

[6] Onder datalekken wordt verstaan: toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens van een organisatie zonder dat dit de bedoeling is.
[7] Onder de WBP was dit het College Bescherming Persoonsgegevens, tegenwoordig de Autoriteit Persoonsgegevens.
[8] Zie bijlage C
[9] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

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 stelt beleid vast en evalueert het.

De principes gaan vooral over de rol van het bestuur bij het waarborgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[10] wordt door de informatiebeveiligingsdienst (IBD) uitgegeven en geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit beeld is tot stand gekomen op basis van een analyse van meldingen aan de IBD, inhoud van lokale rekenkamerrapporten, bevindingen van de visitatiecommissie informatieveiligheid en interviews met gemeentelijke Chief Information Security Officers (CISO). Het is daarmee het document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.6 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[11] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het jaarplan informatiebeveiliging zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

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.

[10] Zie bijlage D

[11] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarplan informatiebeveiliging.

2.5 Reikwijdte informatiebeveiliging

De reikwijdte van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang tot niet openbare gedeelten van de bedrijfsgebouwen.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De gehele informatievoorziening is van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang.
- Informatiebeveiliging is noodzakelijk om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te kunnen waarborgen.
- Het college van B en W is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Velsen hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke Beheersmaatregelen, organisatie-brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening voor de gehele organisatie benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.

Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de leidinggevenden en ziet erop toe dat de leidinggevenden adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De leidinggevenden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet

meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Leidinggevenden dienen erop toe te zien dat de beheersmaatregelen op het verwerken van persoonsgegevens regelmatig worden uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Leidinggevenden voeren quick-scans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:
- Informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
    - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - het dreigingsbeeld gemeenten van de IBD;
    - analyse van de geregistreerde beveiligingsincidenten en datalekken;
    - De door de leidinggevenden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Besluitvorming en stimulering: college van B&W

Het college van B&W is integraal verantwoordelijk voor de beveiliging van de informatievoorziening en heeft daarom een belangrijke rol bij het tot stand brengen en in stand houden van beveiligingsmaatregelen om risico's te minimaliseren. Het college stelt dit beleidsstuk vast maar bespreekt de stand van zaken van de uitvoering in de collegevergaderingen en met het directieteam. Het college vormt zich een mening over de mate waarin zij risico's wil accepteren en treedt handelend op wanneer zij risico's te groot acht om te blijven bestaan. Primair blijft het college op de hoogte via de jaarlijkse ENSIA-rapportage die door de CISO wordt geagendeerd. Hoewel de rapportage bedoeld is voor verantwoording aan de gemeenteraad vormt deze rapportage ook een instrument om het onderlinge gesprek en het gesprek met het directieteam aan te gaan. Daarnaast kunnen signalen van de CISO[12] via de verantwoordelijk portefeuillehouder of eigen waarnemingen aanleiding zijn voor het college om bij te sturen.

3.2 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de leidinggevenden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligings-beleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De

[12] Alleen bij zeer hoge risico's, ernstige beveiligingsincidenten.

directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Velsen gezien als een integraal onderdeel van risicomanagement.

In de praktijk zal de CISO de directie adviseren over bovengenoemde zaken en de coördinatie op zich nemen om de beveiligingsmaatregelen, behorend bij het vastgestelde niveau, te ontwerpen en in werking te krijgen. Dit gebeurt door middel van het uitzetten van taken bij medewerkers met het beheersysteem voor informatiebeveiliging (Key2Control). De taken komen voort uit de acties, geformuleerd in het beveiligingsplan. Met Key2Control worden deze ingepland en wordt de planning bewaakt. Over de voortgang worden de lijnmanagers middels rapportages geïnformeerd zodat ze, zo nodig, zaken kunnen bijsturen.

3.3 Uitvoering: leidinggevenden

Informatiebeveiliging valt onder de verantwoordelijkheden van alle leidinggevenden. De bedoeling is dat alle processen, systemen en gegevens altijd een eigenaar hebben. Er moet dus altijd iemand verantwoordelijk zijn. De leidinggevende die het dichtst op het bedrijfsproces zit kan daar het beste uitvoering aan geven. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. De verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Leidinggevenden rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten.

De CISO stemt, in opdracht van de directie, met de lijnmanager af welke taken gedurende het jaar worden uitgevoerd en door wie. De CISO zorgt voor de coördinatie en de inhoudelijke ondersteuning. De leidinggevende onderneemt actie als zaken bijgestuurd moeten worden.

Taken van de leidinggevenden in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.4 Tweedelijnsondersteuning

De tweede lijn wordt gevormd door ondersteunende professionals, waaronder de Privacy- en Security Officer en informatiemanager. Zij ondersteunen en faciliteren het lijnmanagement bij risico-inventarisaties en de te nemen maatregelen, organiseren campagnes voor bewustwording en leveren ondersteunende beleidsproducten. Om uitvoering te geven aan het beleid wordt de organisatie bijgestaan door adviserende functionarissen die tezamen met de toezichthoudende functionarissen het team informatiebeveiliging en privacy vormen. Op de specifieke onderwerpen wordt dit team aangevuld met specialisten vanuit andere ondersteunende teams.

3.5 Beheersmaatregelen en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Velsen. Het college van B&W en directie zullen volgens de 10 principes voor

informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

3.5.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA[13]-systematiek. Deze is ontwikkeld om de gemeenten in staat te stellen in één keer verantwoording af te leggen aan zowel Rijksministeries als de gemeenteraad over verschillende aandachtsgebieden. De CISO treedt in Velsen op als ENSIA-coördinator. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke leidinggevenden.

De verantwoording over de informatiebeveiliging komt tot uitdrukking door middel van een rapportage. In dit rapport geeft het college van B&W weer hoe de stand van zaken is met betrekking tot informatiebeveiliging in relatie tot het normenkader. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen.

Deze verantwoording stelt de gemeenteraad in staat om haar toezichthoudende rol te vervullen. Zij kan het college aanspreken op geconstateerde tekortkomingen. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Velsen informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

3.5.2 DigiD

DigiD neemt een bijzondere positie in bij de ENSIA-verantwoording. De beheerder van DigiD, Logius, onderdeel van het ministerie van binnenlandse zaken en koninkrijksrelaties, verlangt een onafhankelijk oordeel over de beveiliging van webapplicaties waarop het authenticatiemiddel DigiD wordt ingezet.

Voor DigiD zijn de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

<u>Normen</u>

- De gemeente Velsen conformeert zich aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD versie 3.0.
- Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst.
- Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

<u>Eigenaarschap</u>

- Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de, als systeemeigenaar benoemde, manager eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

<u>Functioneel beheer</u>

- Per DigiD-aansluiting is door de genoemde systeemeigenaar een functioneel beheerder aangesteld die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
- Het auditdossier wordt jaarlijks aan een externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de

[13] *Eenduidige Normatiek Single Information Audit*

dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, t.a.v. DNSSEC) en de beoordeelde releases (C.08).

- Tweemaal per jaar wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag gedaan richting de systeemeigenaar.

Technisch

De gemeente Velsen maakt - voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijke auditor opgestelde - TPM-verklaring verantwoording over aflegt.

3.5.3 Suwinet

Suwinet is een informatiesysteem, betreffende werk en inkomen, over burgers en bedrijven dat wordt beheerd door het Bureau Keteninformatie Werk en Inkomen (BKWI). Over de beveiliging wordt eveneens, door het ministerie van Sociale Zaken en Werkgelegenheid, een onafhankelijk oordeel verlangd. Ook hiervoor wordt een audit-dossier opgebouwd en ter beschikking gesteld aan een externe auditor. Onderdeel van dit dossier is het aansluitbeleid Suwinet dat als uitwerking van dit strategische beleid is opgesteld.

4. De baseline informatiebeveiliging overheid

De komst van de baseline informatiebeveiliging overheid (BIO) betekent gelukkig niet dat we helemaal opnieuw moeten beginnen. Het grootste deel van de baseline informatiebeveiliging gemeenten (BIG) blijft van kracht. De benadering van de BIO is wel anders. Deze gaat meer uit van het hanteren van risicomanagement. De proceseigenaar maakt, op basis van een analyse, de keuze welk beveiligingsniveau passend is voor de processen en de onderliggende informatiesystemen waar hij of zij verantwoordelijkheid voor draagt. Daarmee komt de sturing op informatiebeveiliging door de leidinggevende nadrukkelijker in beeld. Dit hoofdstuk beschrijft nader wat dit betekent en gaat in hoofdlijnen in op de tactische beheersmaatregelen die daarbij een rol spelen. De BIO is gebaseerd op de internationale normen NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017.

4.1 Basis beveiligingsniveaus

In de BIO wordt het begrip basis beveiligingsniveau (BBN) geïntroduceerd. Er worden 3 niveaus onderscheiden. Voor BBN1 ligt de nadruk op “wat mag minimaal verwacht worden?”. Het gaat dan om een minimale set beveiligingsmaatregelen die past bij informatie die niet heel gevoelig of van groot belang voor de bedrijfsvoering is. De maatregelen kom voort uit wet- en regelgeving en algemeen geldende beveiligingsprincipes.
Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe “valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?” Dit niveau is passend voor vertrouwelijke informatie (privacy, commercieel vertrouwelijk) en/of informatie die belangrijk is voor de bedrijfsvoering. Het is tevens van toepassing als incidenten mogelijk leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en/of de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.
BBN3 is van toepassing op gerubriceerde informatie, waarbij weerstand tegen statelijke actoren of vergelijkbare bedreigers nodig is. Dit betreft het hoogste niveau om gegevens die bijzonder gevoelig zijn en/of van cruciaal belang te beveiligen tegen ongeautoriseerde toegang, beschadiging en vernietiging.

Wanneer het BBN is bepaald door de proceseigenaar komen de beheersmaatregelen uit de BIO in beeld welke van toepassing zijn en moeten de operationele beveiligingsmaatregelen in werking worden gesteld die daarbij horen. Veelal zullen dit bekende maatregelen zijn omdat die ook al hoorden bij de BIG-beheersmaatregelen. Het BBN wordt bepaald met het doorlopen van de BBN-toets. Dit is een risico-afweging in de vorm van een vragenlijst (ontwikkeld door de informatiebeveiligingsdienst).

4.2 Verplichte maatregelen

Een deel van de beheersmaatregelen is uitgewerkt in verplichte beveiligingsmaatregelen (in de BIO overheidsmaatregelen genoemd), omdat zij:

- voortvloeien uit *wet- en regelgeving*[14]. Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;
- zo basaal zijn dat zij het *fundament* vormen van een betrouwbare c.q. professionele informatievoorziening;
- dienstbaar zijn aan de beveiliging in een procesketen of -netwerk; niet-naleving door een enkele organisatie is per saldo niet *effectief* voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit niet *efficiënt*. Voor een *generieke dienst* geldt een afweging die analoog is aan het ketenvraagstuk.

In het geval dat een maatregel voor een specifiek geval niet van toepassing *kan* zijn vervalt de verplichting. De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit omvat uitleg volgens het 'pas toe of leg uit' principe. Daarbij worden de daaruit voortvloeiende risico's tevens aangegeven.

4.3 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau

De BIO bepaalt dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd. Uitgaande van het vastgestelde BBN is het niveau bepaald waar de verantwoordelijkheid voor het risicomanagement wordt belegd:

- voor BBN1 is de proceseigenaar volledig verantwoordelijk voor het nemen van (verstandige) beslissingen. Slechts incidenteel en op verzoek informeert deze de CISO over de stand van zaken met betrekking tot zijn BBN1 informatiesystemen.
- voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp/ontwikkelfase) ter consultatie voorlegt aan de CISO.
- voor BBN3 geldt dat vooraf toestemming verleend moet worden door de Gemeentesecretaris voor het verwerken van bijzondere informatie. Voor het verlenen van toestemming is mandatering mogelijk naar bijvoorbeeld de afdelingsmanager Informatiemanagement of CISO.

4.4 Ketensamenwerking en dienstenleveranciers

Binnen de overheid en met andere externe partijen wordt veel in ketens samengewerkt en daarom vormt de gemeenschappelijke veiligheid van informatieketens ook een basis voor de concretisering van overheidsmaatregelen.
Een keten is een samenwerkingsverband tussen organisaties die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) doelstellingen nastreven. Deze ketenpartners zijn zelfstandig, maar zijn ook afhankelijk van elkaar waar het gaat om het bereiken van de gezamenlijke (keten)doelstellingen. Een informatieketen betreft de uitwisseling van informatie binnen zo'n samenwerkingsverband.

In het geval dat een organisatie informatie aan ketenpartners toevertrouwt, blijft deze organisatie er verantwoordelijk voor dat ketenpartners de toevertrouwde informatie zorgvuldig beschermen. De organisatie moet daarom aansluitvoorwaarden eisen of stellen aan de leverende of afnemende partij. Tevens moet de organisatie leveringsgaranties bieden aan de afnemende partij. De organisatie moet hiervoor

[14] *Het gaat dan enkel om de beveiligingseisen die voortvloeien uit wet- en regelgeving. Andere vereisten vallen buiten de reikwijdte van de BIO.*

inzichtelijk hebben van welke informatiesystemen en infrastructuren zij afhankelijk is, welke afhankelijk zijn van haar en hoe het beheer van beiden hierop is ingericht.

In de BIO wordt bij het van toepassing verklaren van beheersmaatregelen en overheidsmaatregelen geen onderscheid gemaakt in interne of externe dienstenleveranciers. Ook bij de wijze waarop verantwoording wordt afgelegd over hun diensten worden interne en externe dienstenleveranciers gelijk behandeld. Dit betekent voor alle dienstenleveranciers het volgende.

- Periodiek leggen alle dienstenleveranciers verantwoording af aan de opdrachtgever bij de overheid.
- De dienstenleveranciers volgen de beveiligingseisen die de overheidsorganisaties of ketenpartners stellen aan de diensten van de dienstenleverancier. Uit efficiëntieoverwegingen kan een dienstenleverancier een standaard beveiligingsniveau aanbieden, maar dit doet geen afbreuk aan de genoemde verantwoordelijkheid van de overheidsorganisaties.
- Voor diensten die aan één organisatie worden aangeboden, legt de dienstenleverancier verantwoording af aan de opdrachtgever.
- Voor diensten die aan meerdere overheden of overheidsonderdelen worden aangeboden stelt de dienstenleverancier één verantwoording op ten behoeve van alle afnemers.

Naast de verantwoording over hun diensten zijn de dienstenleveranciers ook zelf als organisatie gebonden aan informatiebeveiligingsregels. Hierbij is wel een onderscheid aanwezig tussen interne en externe dienstenleveranciers:

- Interne dienstenleveranciers zijn, als onderdeel van de overheid, zelf ook rechtstreeks gebonden aan de BIO. Ze zijn daarmee gehouden aan de reguliere verantwoordings- en toezichtprocedures van de betreffende overheidslagen. De interne dienstenleverancier is ook gebonden aan het jaarlijks opleveren van een In Control Verklaring (ICV). Hierin verklaart de dienstenleverancier dat hij voor zijn eigen bedrijfsvoering aan de BIO voldoet (inclusief de overheidsmaatregelen).
- Externe dienstenleveranciers zijn geen onderdeel van de overheid en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO of het opleveren van een ICV. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd.

4.5 Beheersmaatregelen

De beheersmaatregelen zijn verschillende hoofdstukken ingedeeld, zoals dat ook bij de BIG het geval was. De hoofdstukindeling correspondeert met de ISO27002. Nieuw is dus dat per beheersmaatregel aangegeven is bij welk BBN deze hoort en of het een overheidsmaatregel betreft. De beheersmaatregelen van de BIO zijn ingedeeld in de volgende hoofdstukken:

- Informatiebeveiligingsbeleid (hoofdstuk 5)
- Organiseren van informatiebeveiliging (hoofdstuk 6)
- Veilig personeel (hoofdstuk 7)
- Beheer van bedrijfsmiddelen (hoofdstuk 8)
- Toegangsbeveiliging (hoofdstuk 9)
- Cryptografie (hoofdstuk 10)
- Fysieke beveiliging en beveiliging van de omgeving (hoofdstuk 11)
- Beveiliging bedrijfsvoering (hoofdstuk 12)
- Communicatiebeveiliging (hoofdstuk 13)
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen (hoofdstuk 14)
- Leveranciersrelaties (hoofdstuk 15)
- Beheer van informatiebeveiligingsincidenten (hoofdstuk 16)
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (hoofdstuk 17)
- Naleving (hoofdstuk 18)

4.5.1 Informatiebeveiligingsbeleid

Er is beleid nodig om informatiebeveiliging succesvol onderdeel te laten zijn van de bedrijfsvoering. Het biedt de directie een instrument om dit aan te sturen. Het beleid moet voldoende kwaliteit hebben en aansluiten bij de actualiteit. Evaluatie dient daarom regelmatig plaats te vinden.

4.5.2 Organiseren van informatiebeveiliging

Informatiebeveiliging ontstaat niet vanzelf en moet dus worden georganiseerd. Rollen en verantwoordelijkheden moeten helder zijn en er moet deskundige ondersteuning aanwezig zijn.

4.5.3 Veilig personeel

Om veilig te werken met de informatievoorziening moeten medewerkers aan (integriteits-)eisen voldoen en voldoende geëquipeerd zijn. Dat begint al voorafgaand aan de daadwerkelijke indiensttreding, waarbij wordt onderzocht of er mogelijk redenen zijn om de beoogde medewerker de toegang te ontzeggen. Arbeidsvoorwaarden, opleiding en training waarborgen dat bij de medewerkers voldoende bewustzijn is van de risico's die samenhangen met het werken met gegevens van de overheid. Daarbij dient de werkgever disciplinaire procedures te hebben ingericht als er, vanwege schendingen, moet worden opgetreden. Dit geldt zowel voor eigen medewerkers als voor ingehuurd personeel en externe gebruikers.

Bij beëindiging of wijziging van het dienstverband gaat het om het bewerkstelligen dat betrokkenen de organisatie, vanuit het oogpunt van informatiebeveiliging, ordelijk verlaten dan wel dat wijziging van het dienstverband ordelijk verloopt.

4.5.4 Beheer van bedrijfsmiddelen

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen en dienen beschermd te worden. Van belang is dat alle relevante bedrijfsmiddelen bekend, geregistreerd en voorzien zijn van een eigenaar en duidelijk is wie verantwoordelijk is voor het handhaven van geschikte beveiligingsmaatregelen. Een categorie die daarbij speciale aandacht verdient wordt gevormd door de verwijderbare media zoals usb-sticks, geheugenkaartjes, externe harde schijven en back-upmedia. Ook de media die niet langer nodig is en dus moet worden afgevoerd verdient een zorgvuldige behandeling.

Gegevensclassificatie naar de mate van beschikbaarheid, integriteit en vertrouwelijkheid is belangrijk om de juiste beveiligingsmaatregelen toe te passen. Het heeft weinig zin om gegevens die van minder belang zijn zwaar te beveiligen. Dat brengt onnodige moeite en kosten met zich mee. Aan de andere kant moeten gegevens die van groot belang en/of van gevoelige aard zijn uiteraard wel goed worden beschermd. De eigenaar van de gegevens bepaalt het niveau van classificatie en houdt daarbij eveneens rekening met wettelijke eisen.

4.5.5 Toegangsbeveiliging

Logische toegangsbeveiliging is het geheel aan maatregelen met als doel de toegang tot gegevens en informatiesystemen te beheersen, zodat gegevens, informatiesystemen en hulpmiddelen worden beschermd tegen ongeautoriseerde handelingen. Belangrijke aandachtsgebieden zijn**:**

- het definieren van toegangsbeleid waarin is aangegeven aan welke bedrijfseisen de toegangsbeveiliging moet voldoen en waarbij rekening gehouden wordt met afzonderlijke bedrijfstoepassingen. Tevens wordt rekening gehouden met toegang via externe werkplekken (thuiswerkplek) en via mobiele apparatuur;

- het beheer van de toegangsrechten van gebruikers binnen de gemeente en het voorkomen van onbevoegde toegang tot informatiesystemen;
- de verantwoordelijkheid van gebruikers om zorgvuldig om te gaan met hun wachtwoorden en om onbeheerde gebruikersapparatuur passend te beschermen;
- de gebruikerstoegang tot netwerken en netwerkdiensten (denk aan internet) waarbij de veiligheid van het gemeentelijk netwerk en bijbehorende netwerkdiensten niet in gevaar komt;
- het treffen van beveiligingsvoorzieningen bij het inloggen om onbevoegde toegang tot informatiesystemen te voorkomen;
- het afschermen van (hulp)programmatuur die toegang geeft tot informatie (denk aan query tooling (programma's om gegevens uit databases op te vragen), maar ook snelkoppelingen) tegen onbevoegd gebruik;
- het waarborgen van de informatiebeveiliging bij het gebruik van telewerken en/of mobiele apparatuur.

4.5.6 Cryptografie

Cryptografie ofwel het versleutelen van gegevens wordt toegepast om te bewerkstelligen dat die alleen door bevoegde functionarissen kunnen worden gelezen. Zo worden bijvoorbeeld de gegevens die via het internet lopen standaard versleuteld zodat ze onderweg niet kunnen worden afgeluisterd of gewijzigd. Het doel is de bescherming van de vertrouwelijkheid, authenticiteit en/of integriteit te beschermen. Er moet bepaald worden in welke gevallen cryptografische beveiligingsmaatregelen worden ingezet en voor welk type encryptie er gekozen wordt. Voor de encryptie en het weer leesbaar maken van de gegevens dient men te beschikken over een sleutel. Gezien het belang is zorgvuldig beheer van deze sleutels noodzakelijk.

4.5.7 Fysieke beveiliging en beveiliging van de omgeving

Fysieke beveiliging is gericht op het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein, de informatie van de organisatie, bedrijfsmiddelen én het voorkomen van de 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, computerruimte, etc).
Een ander aandachtsgebied is het naleven van een clear desk en clear screen beleid, ofwel ervoor zorgdragen dat elke werkplek na werktijd is opgeruimd (gevoelige en bedrijfs-kritische informatie op papier en verwijderbare opslagmedia), dat computerapparatuur is uitgeschakeld en dat sprake is van schermbeveiliging bij het tijdelijk verlaten van de werkplek.

4.5.8 Beveiliging bedrijfsvoering

Beveiliging van de bedrijfsvoering omvat alle ICT-gerelateerde maatregelen om de informatievoorziening te beschermen tegen verstorende invloeden. Belangrijke maatregelen zijn o.a. de bescherming tegen kwaadaardige software en digitale inbraak en het maken van reservekopieën (back-up). Daarnaast het toepassen van procedures om op een gecontroleerde wijze problemen op te lossen en wijzigingen door te voeren op de ICT-voorziening.

Ondanks beschermende maatregelen is het nog steeds mogelijk dat er verstorende invloeden plaatsvinden, al dan niet door kwaadwillende personen geïnitieerd. Daarvoor is het nodig om de ICT-voorziening te testen en te bewaken. Met penetratietesten wordt de

weerbaarheid in kaart gebracht en eventuele kwetsbaarheden opgespoord. Een continu monitoringsysteem dient om ongewenste gedragingen te detecteren.

Preventieve en detectie-maatregelen tezamen kunnen geen 100% veiligheid bieden. Er moeten ook zaken hersteld kunnen worden na een incident en er moeten dus recente reservekopieën (back-ups) voorhanden zijn van de gehele informatievoorziening.

Hackers en kwaadaardige software maken vaak gebruik van programmatuurfouten in software. Deze fouten worden door de softwareontwikkelaar opgelost en via updates aangeboden. Met een strak updateregime wordt de aanvaller een belangrijk wapen uit handen geslagen.

4.5.9 Communicatiebeveiliging

Transport van gegevens over netwerken, zowel intern als over internet moet worden beveiligd om ongewenste modificatie en ongeautoriseerde inzage tegen te gaan. Het is daarbij ook nodig om het interne netwerk in logische eenheden te scheiden. Bij elke eenheid kan dan voor een passend beveiligingsniveau gezorgd worden.

Bij transport over internet is vooral de inzet van sterke cryptografie noodzakelijk. Aangezien er dan veelal wordt gecommuniceerd met externe partijen is het nodig om afspraken over de wijze waarop dit gebeurt, de omgang met de gegevens en geheimhouding in overeenkomsten vast te leggen.

4.5.10 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Dit onderdeel gaat met name in op de beveiliging van informatiesystemen en het onderhoud op deze informatiesystemen. Informatiesystemen omvatten besturingssystemen, infrastructuur, bedrijfstoepassingen en toepassingen die ten dienste staan van de gebruikers. Belangrijke aandachtsgebieden zijn:

- het opnemen van het thema informatiebeveiliging in de inkoopprocedure ingeval van aanschaf van nieuwe informatiesystemen of onderdelen ervan;
- principes om bij de systeemontwikkeling beveiliging onderdeel te laten zijn van het ontwerp;
- het afschermen van alle operationele programmatuur en systeembestanden voor onbevoegde wijzigingen;
- het zorgvuldig kiezen, beschermen en beheersen van testgegevens. Het anonimiseren van persoonsgegevens en het aanpassen of onherkenbaar maken van gevoelige informatie wordt hierbij in acht genomen;
- het implementeren van wijzigingen via een formele procedure wijzigingsbeheer om het risico van storingen of/of fouten zoveel mogelijk te voorkomen;

Veel beheersmaatregelen in dit hoofdstuk gaan over softwareontwikkeling. De gemeente Velsen schaft standaardproducten aan en ontwikkelt dus zelf geen software en laat deze niet ontwikkelen. Bij de selectie van standaardsoftware is het echter wel van belang om ingebouwde beveiligingsmaatregelen zwaar mee te laten wegen.

4.5.11 Leveranciersrelaties

In dit hoofdstuk gaat het erom bedrijfsmiddelen van de organisatie, die toegankelijk zijn voor externe leveranciers te beveiligen. Dit speelt met name bij gebruik van softwaretoepassingen die op het internet worden aangeboden (Cloud-computing). Als gevolg daarvan komen gegevens van Velsen op externe servers te staan en is er geen directe invloed op de beveiliging meer mogelijk.

Om de gegevensbeveiliging dan toch onder controle te houden is het nodig om in overeenkomsten afspraken te maken over gestelde eisen. Nadat de overeenkomst tot stand is gekomen dient er gecontroleerd te worden of de afspraken door de leveranciers worden nageleefd.

Wijzigingen in de dienstverlening worden beoordeeld op consequenties voor de gegevensbeveiliging. Zo nodig worden overeenkomsten aangepast om de beveiliging dan op een voldoende hoog niveau te houden.

4.5.12 Beheer van informatiebeveiligingsincidenten

Een beveiligingsincident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden en kan leiden tot financiële, imago en/of politieke schade. Het doel is om het aantal beveiligingsincidenten zoveel mogelijk te voorkomen en indien een incident zich voordoet de schade zo beperkt mogelijk te houden. Belangrijk is dat een incident wordt gemeld bij de juiste personen (leidinggevende, CISO, Functionaris Gegevensbescherming).

Hiervoor is een formele procedure nodig waarin is aangegeven hoe de gemeente Velsen omgaat met het beheer van beveiligingsincidenten. Dan gaat het over het signaleren, registreren, analyseren van incidenten en het voorkomen van escalatie (crisisbeheersing), het afhandelen van incidenten en het periodiek rapporteren over de stand van zaken. Tijdens het optreden van het incident dient er aandacht te zijn voor het verzamelen en bewaren van informatie die als bewijs kan dienen van kwaadwillende activiteiten. Alle medewerkers en externe gebruikers zijn op de hoogte van deze procedure.
Uit de registratie van incidenten kan lering worden getrokken om maatregelen te treffen die de kans op herhaling beperken.

Hierbij is ook aandacht nodig voor interne en externe communicatie ingeval sprake is van een hoge escalatie (gemeente overstijgend).

4.5.13 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Bij continuïteitsbeheer gaat het om maatregelen die gericht zijn op het tegengaan van onderbreking van bedrijfsactiviteiten bij de gemeente Velsen, op het beschermen van kritieke bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en op het bewerkstelligen van tijdig herstel. Bedrijfscontinuïteit gaat verder dan alleen informatiebeveiliging maar de beschikbaarheid van de informatievoorziening is wel cruciaal voor het kunnen voortzetten of herstellen van bedrijfsprocessen.

Continuïteitsplannen waaronder uitwijkmogelijkheden en het periodiek testen en evalueren van deze plannen spelen hierbij een belangrijke rol.

4.5.14 Naleving

In dit onderdeel ligt de nadruk erop schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen te voorkomen. Er zijn vele wetten en regelgeving van toepassing op de gemeente zoals de BRP, PUN, BAG en SUWI, maar een bijzondere is de naleving van de Europese privacy wetgeving[15].

[15] *General Data Protection Regulation of Algemene Verordening Gegevensbescherming.*

Een ander belangrijk punt is dat de gemeente Velsen voldoet aan de gestelde licentie-eisen op programmatuur om eventuele toekomstige boetes/claims van leveranciers te voorkomen.

Om de naleving te toetsen dient er te worden gecontroleerd. Dit kan worden gedaan door een interne of externe auditor. Naleving van het vastgestelde technische beveiligingsniveau vindt plaats door gespecialiseerde testen[16]

[16] *Penetratietesten, kwetsbaarheidsanalyses.*

5. Kritieke processen

5.1 Welke zijn de kritieke processen van de gemeente Velsen?

In 2016 zijn de meest kritieke processen van de gemeente Velsen vastgesteld door het college van Burgemeester en Wethouders. De focus van informatiebeveiliging is hiermee op deze processen komen te liggen. Dat betekent onder meer dat de gebruikte gegevens geclassificeerd zijn, er extra beheersing van en controle op autorisaties van de ondersteunende systemen is ingevoerd en het toezicht op eventuele leveranciers van software-oplossingen buiten het gemeentehuis wordt verstevigd. Voor de overige processen geldt dat het goed is hier ook voldoende aandacht aan te besteden maar het risico op beveiligingsincidenten met een grote impact wordt als aanzienlijk minder ingeschat. De belangrijkste risico's worden door generieke beveiligingsmaatregelen al geminimaliseerd.

Op basis van de volgende criteria zijn de kritieke processen vastgesteld:

- Er is een wettelijke termijn waarbinnen het proces beschikbaar moet zijn.
- Verstoring of uitval heeft direct impact op de bedrijfsvoering.
- Verstoring of uitval heeft direct impact op de dienstverlening van de organisatie.
- Door verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid loopt de organisatie imagoschade op.
- Verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid levert schade op bij andere partijen.
- Verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid brengt een aanzienlijke kostenpost met zich mee.

De kritieke processen van Velsen zijn:

- Beheer basisregistraties
- Belastingheffing en inning
- Dienstverlening Burgerzaken
- Dienstverlening Sociaal Domein
- Financiële administratie
- Bedrijfsprocessen openbare orde en veiligheid
- Vergunningverlening
- Beheer personeelszaken