1.Inleiding

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente Velsen[1]. Immers de gemeente is in de kern een informatiehuishouding, beheert veel persoons- en privacy gevoelige gegevens en behoort uit dien hoofde 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 op (de continuïteit van) de bedrijfsvoering en tot imagoschade met mogelijke politieke gevolgen.

Vanuit de overheid is de belangstelling en noodzaak voor informatieveiligheid de afgelopen 2 jaren enorm toegenomen. Dit vanwege de alsmaar toenemende bedreigingen zoals cybercriminaliteit maar ook diverse ernstige beveiligingsincidenten zoals DigiNotar en Ddos aanvallen. Daarmee is de kwetsbaarheid van de IT-infrastructuur bij gemeenten op een duidelijke wijze aangetoond en heeft dit als het ware geleid tot een soort wake-up-call. Immers, beveiligingsincidenten kunnen het vertrouwen in de overheid ernstig schaden.

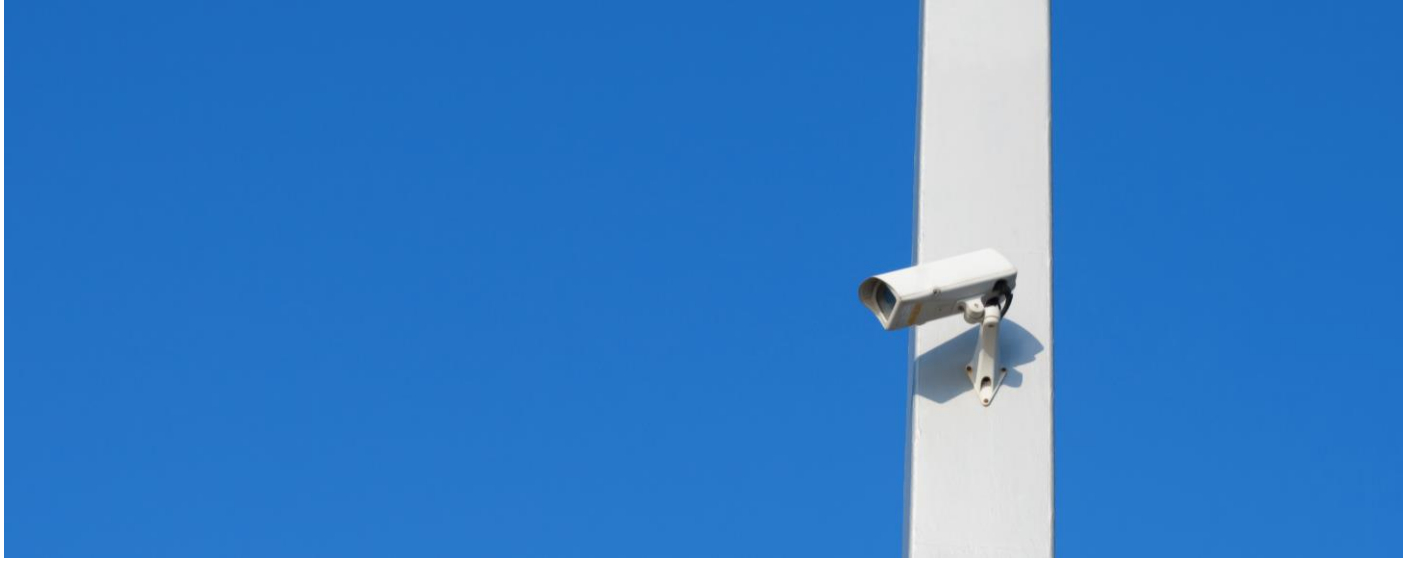
Mede als gevolg hiervan is in 2012 de Informatiebeveiligingsdienst voor gemeenten (IBD) onder de vlag van de Vereniging Nederlandse Gemeenten (VNG) opgericht en is de resolutie informatieveiligheid tijdens de bijzondere algemene ledenvergadering (BALV) in november 2013 door de leden bekrachtigd. In deze resolutie staat onder meer dat informatieveiligheid opgenomen wordt in de portefeuille van een van de leden van het college van B&W en dat de Baseline Informatiebeveiliging Gemeenten (BIG) het gemeentelijke basisnormenkader voor informatieveiligheid wordt. Voorts is in deze resolutie aangegeven dat gemeenten informatieveiligheid bestuurlijk en organisatorisch borgen en informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners.

Het college van B&W van de gemeente Velsen heeft in 2011 voor het eerst beleid op het gebied van informatieveiligheid vastgesteld. Dit beleid wordt thans herzien waarbij nu aansluiting wordt gemaakt met de resolutie van de VNG en de gemeente Velsen de BIG als gemeentelijk basisnormenkader opneemt in haar beleid.

Het hiervoor liggende beleidsdocument geeft de kaders en uitgangspunten weer om informatieveiligheid over de periode 2016-2019[2] op een professionele wijze te borgen in de organisatie van de gemeente Velsen. Het gaat dan om de introductie van een information security managementsysteem (ISMS) ofwel een informatiebeveiligingsmanagementsysteem. Een ISMS[3] is de 'motor' van de informatiebeveiligingsactiviteiten die een gemeente behoort te nemen vanuit een plan-

[1] Citaat Kwaliteitsinstituut Nederlandse Gemeenten.
[2] Periode conform tactische BIG, hoofdstuk 5
[3] In dit beleidsdocument hanteren we de terminologie van de IBD en spreken we in het vervolg over een ISMS.

do-check-act cyclus. Het doel van een ISMS is onder andere het continu beoordelen welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen.
Om een ISMS te realiseren is vanaf augustus 2014 een projectgroep ingesteld en is inmiddels volgens de aanpak van de IBD duidelijk welke activiteiten op korte termijn gerealiseerd moeten worden. De bedoeling is dat periodiek de stand van zaken wordt geëvalueerd en waar nodig wordt bijgesteld. Overdracht van het ISMS naar de organisatie zal plaatsvinden nadat de organisatie rond het beheer van het ISMS staat en voldoende geëquipeerd is om de daarbij behorende taken naar behoren te kunnen uitvoeren.



2.1 Visie op informatiebeveiliging

De komende jaren zet de gemeente Velsen in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie 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.[4] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

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 nieuwe, innovatieve manieren van 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.[5]

2.2 Definitie van informatiebeveiliging

Informatiebeveiliging is het samenhangend geheel van beheersingsmaatregelen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie garandeert. Daar waar gesproken wordt over informatie geldt dit ook voor de onderliggende gegevens.

Het begrip 'informatiebeveiliging' heeft aldus betrekking op:
- *beschikbaarheid:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *integriteit:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- *vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Voorkomende beheersingsmaatregelen zijn:

[4] Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.

[5] Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de gemeente Velsen verricht.

- preventie: gericht op het voorkomen van een gebeurtenis door bijvoorbeeld encryptie van data of functiescheiding;
- detectie: gericht op het vaststellen van een fout, nalatigheid of kwaadwillende actie door bijvoorbeeld detectiemethodieken;
- repressie: bedoelt om de gevolgen van een incident te beperken, bijvoorbeeld het maken van een back-up, uitwijkomgeving;
- correctie: gericht op het corrigeren van opgetreden gebeurtenissen door bijvoorbeeld het terugzetten van een back-up gevolgd door het opnieuw doorvoeren van transacties.

2.3 Doel beleid

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Velsen 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 SMART-planning[6]
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, zie paragraaf 2.4).

2.4 Doelgroep

Het college van Burgemeester en Wethouders, directie en lijnmanagement draagt de inhoud uit naar alle medewerkers en gebruikers die zijn betrokken bij de verwerking en beheer van informatie en/of het beheer van informatiesystemen, waarvan de verantwoordelijkheid bij de gemeente Velsen ligt. Het informatiebeveiligingsbeleid is van toepassing voor alle medewerkers en gebruikers.

2.5 Reikwijdte en afbakening

De scope 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 en gebruikte systemen c.q. applicaties.

Informatiebeveiliging 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, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar vooral ook mensen en processen. Het is dan ook niet alleen het domein van de afdeling informatiemanagement. Ook zaken als toegangsbeveiliging, beveiliging van personeel en bureau horen tot het domein van informatiebeveiliging.

Informatiebeveiliging heeft als aandachtsgebieden:
- Organisatie: verantwoordelijkheden, rapportages, sturing, communicatie, coördinatie, bewustzijn, de houding en het gedrag van medewerkers;

[6] SMART = specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden

- Facilitaire beveiliging: toegangsbeveiliging, inbraakbeveiliging, kantoren en stroomvoorziening;
- ICT-beveiliging: applicaties, netwerken, back-up systemen en beheerprocedures.

2.6 Grondslagen

Dit beleid is gebaseerd op de volgende wet- en regelgeving
- Het informatiebeveiligingsbeleid van Velsen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
- Het beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) die is afgeleid van de code voor informatiebeveiliging (NEN/ISO 27002).

Het gemeentebrede informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Hierbij geldt specifieke wet- en regelgeving waar altijd aan voldaan moet worden, zoals de Wet bescherming persoonsgegevens (WBP), de Basisregistratie personen (BRP), Paspoort uitvoeringsregeling Nederland (PUN), de Basisregistratie adressen en gebouwen (BAG), de archiefwet, het Reglement Rijbewijzen en Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI).

Indien hogere beveiligingseisen worden gesteld vanuit bepaalde kerntaken op grond van wet- en regelgeving dan worden deze eisen geïmplementeerd bovenop de eisen van de BIG.

2.7 Uitgangspunten

Bij de organisatieontwikkeling van Velsen staan vier succesfactoren centraal: attent, betrouwbaar, doelgericht en dynamisch. Informatiebeveiliging is vooral belangrijk om succes te boeken op de factoren betrouwbaar en doelgericht en daarvoor hanteert Velsen de volgende uitgangspunten:
- Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor een efficiënte en effectieve bedrijfsvoering. Omdat de gemeente Velsen onderdeel uitmaakt van de totale federatieve overheid en ook verbonden is met andere ketenpartijen, heeft een onveilige situatie bij de gemeente Velsen direct gevolgen voor de veiligheid van andere overheden of partijen.
- Informatiebeveiliging is noodzakelijk om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te kunnen borgen.
- De informatiebeveiligingstaken moeten als integraal onderdeel van de dagelijkse bedrijfsvoering in de organisatie belegd worden.
- Informatiebeveiliging is niet vanzelfsprekend en moet georganiseerd worden. Het vergroten van het bewustzijn van medewerkers over informatiebeveiliging vraagt continue aandacht van het management.
- Informatiebeveiliging is een cyclisch proces. Omdat er steeds nieuwe bedreigingen en risico's ontstaan en de eisen vanuit wet- en regelgeving in de tijd kunnen veranderen, moet het informatiebeveiligingsbeleid periodiek geactualiseerd worden. Om te kunnen bepalen wat de bedreigingen met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zijn, worden risicoanalyses uitgevoerd. Om de controle en de kwaliteit te waarborgen wordt informatiebeveiliging in de planning en control cyclus opgenomen. Een onafhankelijke controle is nodig om vast te stellen of de informatiebeveiliging voldoet aan het informatiebeveiligingsbeleid, respectievelijk of de uitgevoerde maatregelen voldoende zijn om het gewenste niveau van informatiebeveiliging te bewerkstelligen.
- Informatiebeveiliging moet bij voorkeur informatiebeveiligingsincidenten voorkomen, respectievelijk de effecten van het optreden van incidenten beperken.

- Informatiebeveiligingsmaatregelen mogen niet ten koste gaan van de veiligheid van eigen personeel en van derden.
- Het gewenste informatiebeveiligingsniveau wordt vastgelegd in de vorm van minimumeisen. Op basis van wet- en regelgeving, overeenkomsten met andere overheden en derden, of bij bijzonder kwetsbare en vitale componenten van de informatievoorziening, kan op onderdelen een hoger niveau van informatiebeveiliging gelden.
- Medewerkers hebben een eigen verantwoordelijkheid voor hun gedrag binnen de gestelde normen en eisen en spreken elkaar aan op onveilig gedrag. Ook signaleren zij mogelijke hiaten en melden deze direct aan de leidinggevenden. Velsen heeft vertrouwen in haar medewerkers, mede gebaseerd op het aannamebeleid, de geldende procedures en de uit te voeren controles. Alle medewerkers hebben een eed/belofte afgelegd, of (zo nodig) een geheimhoudingsverklaring getekend. Medewerkers moeten bekwaam zijn in het uitvoeren van de functietaken en in dat kader de benodigde opleidingen gevolgd hebben. Er heerst een cultuur van bewustzijn en constante alertheid met betrekking tot (on)veilig gedrag en nieuwe bedreigingen.
- Personen krijgen niet meer autorisaties dan nodig is voor het uitvoeren van een taak.

2.8 Privacy en persoonsgegevens

De beveiliging van persoonsgegevens en bescherming van privacy (beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking) van burgers is een van de speerpunten van de gemeente Velsen. Persoonsgegevens worden gezien als een bijzondere soort van informatie en bij de verwerking van dit type gegevens speelt privacybescherming en de daarvoor geldende wetgeving een essentiële rol. Het gaat dan om de wet Basisregistratie Personen (BRP) en Wet bescherming persoonsgegevens (Wbp).

- De wettelijke grondslag voor gegevensverwerking in de basisregistratie personen is de BRP en niet de Wbp.
- De Wbp is van toepassing op alle registraties van persoonsgegevens die aanvullend zijn op de BRP.
- Het College bescherming persoonsgegevens (CBP) kan het college van B&W aanspreken op het niveau van de maatregelen voor de beveiliging van de verwerking van persoonsgegevens en de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.
- Informatiesystemen zijn verplicht om daar waar ze persoonsgegevens gebruiken deze rechtstreeks uit de BRP te halen.
- Toegang tot de informatie uit de BRP, ongeacht het gebruikte informatiesysteem, moet altijd vooraf door de gegevenseigenaar[7] van de BRP worden getoetst en goedgekeurd.
- Ingeval van een datalek omtrent persoonsgegevens wordt dit gemeld aan het CBP.
- De gemeente Velsen maakt waar nodig gebruik van een privacy impact assessment om de mate van impact en benodigde beveiligingsmaatregelen vast te stellen.

2.9 Risicobenadering

De gemeente Velsen volgt een aanpak van informatiebeveiliging op basis van risicobeheersing. Immers honderd procent beveiliging is een utopie en zou ook zeer belastend zijn voor de organisatie wat ongewenst is. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van

[7] Gegevenseigenaar is verantwoordelijk voor de juistheid van de gegevens in het informatiesysteem in kwestie

beveiligingsmaatregelen te implementeren en in staat daarbij een betere afweging tussen kosten en noodzaak te maken.

Vanuit een nulmeting op basis van de BIG wordt bepaald hoe groot het 'gat' is tussen hetgeen nodig is en van waaruit de gemeente vertrekt. Vervolgens vindt op basis hiervan 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 gegevenseigenaar de kwetsbaarheid van het werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident. Hierbij houdt hij rekening met de beschermingseisen ten aanzien van de informatie.

2.10 Samenwerking

Intergemeentelijke samenwerking en het samenwerken met ketenpartners zal er toe leiden dat er steeds vaker informatie wordt uitgewisseld met samenwerkingspartners. De huidige ontwikkelingen in de drie decentralisaties van zorgtaken zijn hiervan een sprekend voorbeeld. Met deze samenwerkingspartners worden afspraken gemaakt over het vereiste niveau van informatiebeveiliging die de gemeente Velsen stelt. In sommige gevallen kan dit hoger liggen dan de vereisten volgens de BIG. Denk in dat geval aan privacygevoelige gegevens.

2.11 Werking

Dit beleid heeft betrekking op de periode 2016-2019[8] en treedt in werking na vaststelling door het college van B&W. Daarmee komt het oude beleid voor informatiebeveiliging van de gemeente Velsen uit 2011 te vervallen.

[8] Periode conform Tactische BIG, hoofdstuk 5

3.1 Interne organisatie

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

3.2 Verantwoordelijkheden

Voor een goede borging van informatiebeveiliging is het noodzakelijk dat verantwoordelijkheden helder zijn belegd.

- Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente.
  - stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;

- De Directie is ambtelijk verantwoordelijk voor de beveiliging van informatie en daarbij behorende algemene sturing:
  - stuurt de organisatie aan op beveiligingsrisico's;
  - controleert of de getroffen maatregelen overeenstemmen met de beveiligingseisen en of deze voldoende bescherming bieden;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.

- Het lijnmanagement[9] is verantwoordelijk voor de integrale beveiliging van de organisatieonderdelen:
  - stelt op basis van een expliciete risicoafweging beveiligingseisen vast volgens de classificatie voor zijn informatiesystemen;
  - is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit deze eisen;
  - stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - meldt incidenten en rapporteert in hoeverre hun organisatieonderdeel het informatiebeveiligingsbeleid van de gemeente naleeft.

[9] Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan dit een afdelingsmanager of een teamleider zijn maar ook de griffier.

- De gemeentelijke Service Organisatie (Informatiemanagement, HR, Algemene zaken (facilitair), etc.) is verantwoordelijk voor de uitvoering van:
  - de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT aangelegenheden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, logging van activiteiten en backup & recovery;
  - maatregelen gericht op beveiliging van personeel zoals screening, geheimhoudingsverklaringen en bewustwordingsprogramma's;
  - maatregelen gericht op beveiliging van gebouwen, publieke en werkruimten van de gemeente;
  - het opzetten en beheren van een ISMS.

3.3 Taken en rollen

Het college van B&W stelt formeel het informatiebeveiligingsbeleid vast, delegeert de uitvoering hiervan aan de directie en informeert de raad over dit thema. Binnen het college van B&W valt informatiebeveiliging onder de portefeuille informatiemanagement. De directie adviseert het college van B&W formeel over vast te stellen beleid.

Namens de directie geeft de afdelingsmanager informatiemanagement (AMIM) op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan. De hieruit voortvloeiende taken op het gebied van informatiebeveiliging zijn binnen de afdeling Informatiemanagement belegd bij de coördinator informatiebeveiliging (CIB).

De coördinator informatiebeveiliging:
- heeft een coördinerende rol en is centraal aanspreekpunt voor alle aangelegenheden op het gebied van informatiebeveiliging binnen de gemeente;
- onderhoudt contacten met externe partijen (zoals IBD) om onder meer op de hoogte te blijven van de ontwikkelingen op het gebied van informatiebeveiliging;
- ondersteunt de directie en afdelingen en geeft indien nodig advies op het gebied van informatiebeveiliging;
- houdt de registratie bij van alle gemelde beveiligingsincidenten en draagt zorg voor een juiste afhandeling;
- stelt het informatiebeveiligingsplan op en onderhoudt dit plan jaarlijks;
- implementeert het door de directie goedgekeurde informatiebeveiligingsplan en voert hierop voortgangsbewaking uit;
- evalueert en rapporteert periodiek aan de directie over de bevindingen en stand van zaken.

Vanuit de afdeling Algemene Zaken is een privacyfunctionaris belast met de implicaties die voortvloeien uit de Wbp ofwel op de bescherming van de privacy en persoonsgegevens binnen de gemeente Velsen. Het gaat dan onder meer over het informeren, adviseren en toezien op de naleving en uitvoering van privacy impact

assessments (PIA). De werkzaamheden van de privacyfunctionaris zijn afgestemd met die van de coördinator informatiebeveiliging.

Voor de afdelingen c.q. werkeenheden waar zich kritische bedrijfsprocessen (zie hoofdstuk 5) afspelen zijn contactpersonen informatiebeveiliging benoemd. Daarnaast zijn er afdelingen/werkeenheden die taakgebieden behartigen waar de BIG zich specifiek op richt: personeelszaken, fysieke beveiliging en ICT-diensten en infrastructuren. Ook daar worden contactpersonen benoemd. In de huidige organisatieopzet gaat het om de afdelingen:

- Maatschappelijke ontwikkeling,
- Werk, Inkomen en Zorg,
- Financiën,
- Algemene Zaken,
- Human Resources,

en om de werkeenheden:

- Ruimtelijke informatie,
- Ruimte en informatie,
- Burgerzaken,
- Belastingen en invordering,
- Facilitaire diensten,
- Automatisering,
- Vergunningen.

Zij zijn aanspreekpunt voor de coördinator informatiebeveiliging om:

- uitvoering van maatregelen die per afdeling of specifiek voor één afdeling getroffen moeten worden te beleggen en te plannen.
- gezamenlijk op te treden om de negatieve gevolgen van incidenten op de informatievoorziening van één of meerdere afdelingen te beperken.

In een aantal gevallen kan een medewerker contactpersoon voor meerdere afdelingen/werkeenheden zijn. Periodiek voert de coördinator informatiebeveiliging overleg met deze contactpersonen en eventueel andere aan informatiebeveiliging gerelateerde medewerkers (denk aan privacy gerelateerde activiteiten) over de stand van zaken en nieuwe ontwikkelingen op het gebied van informatiebeveiliging. De resultaten hiervan neemt de coördinator informatiebeveiliging mee in zijn evaluatie.

Het onderwerp Informatiebeveiliging is een vast onderdeel op de agenda van het lijnoverleg zodat er sturing plaatsvindt op de uitgevoerde activiteiten.

Controle op de werking van de vastgestelde beveiligingsmaatregelen ligt bij Concern Control en zij informeert tijdig de coördinator informatiebeveiliging over de daaruit voortkomende bevindingen.

3.4 Rapportages

De coördinator informatiebeveiliging stelt rapportages op naar aanleiding van wettelijke verplichtingen en incidenten en de frequentie sluit zoveel mogelijk aan op de P&C cyclus van de gemeente. Afhankelijk van het type rapportage worden deze besproken en afgestemd met de betrokkenen en verantwoordelijken.

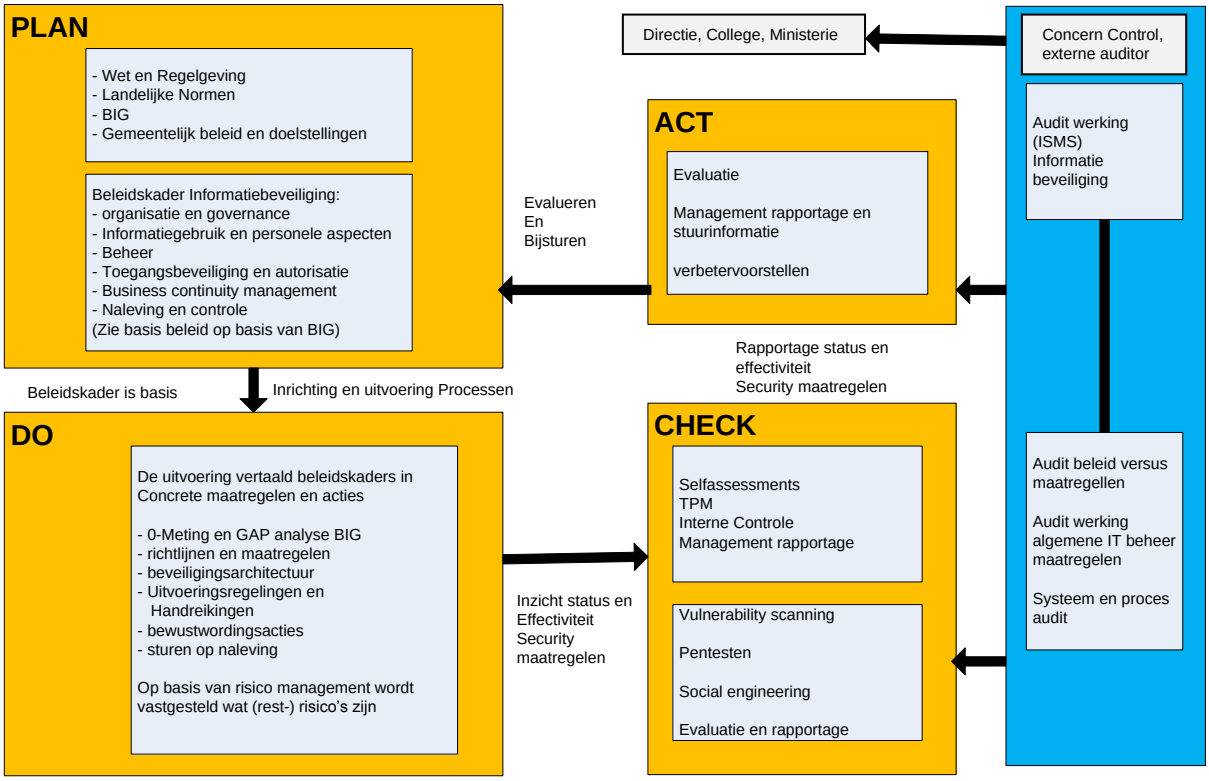
3.5 ISMS

Een ISMS is een managementsysteem dat de gemeente Velsen inzicht geeft in de stand van zaken en op een gestructureerde wijze houvast biedt om verdere verbeteringen op het gebied van informatiebeveiliging door te kunnen voeren. Het hebben van een ISMS is niet een eenmalige activiteit. Het is een voortdurend proces dat binnen de gemeente behoort te worden uitgevoerd. Het doel van het ISMS is onder andere het continu beoordelen welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen.

Het beheer van het ISMS van de gemeente Velsen ligt bij de coördinator informatiebeveiliging. Hij zorgt ervoor dat alle noodzakelijke activiteiten (met bijbehorende documentatie) op een deugdelijke wijze zijn vastgelegd, waardoor het mogelijk is om achteraf de werking van dit systeem te kunnen aantonen (aantoonbaar in control zijn).

Een ISMS is gebaseerd op een set van periodieke activiteiten die is onderverdeeld in een verbetercyclus plan-do-check-act (PDCA-cyclus) welke idealiter aansluit op de P&C cyclus van de gemeente. Deze activiteiten zijn verdeeld over de taken en rollen zoals opgenomen in de beveiligingsorganisatie.

Als voorbeeld is een PDCA-cyclus in relatie tot een ISMS hieronder weergegeven:



Information Security Management System

Een korte toelichting hierop is als volgt:

Plan

In de PLAN-fase vindt in het eerste jaar vorming plaats van het ISMS en stelt het college van B&W het gemeentelijk informatiebeveiligingsbeleid vast. Voorts vindt doorvertaling van dit beleid plaats naar een informatiebeveiligingsplan. In dat plan staan de activiteiten

voor het komende jaar gepland met de daarbij benodigde middelen (capaciteit en budget).

DO

In de DO-fase vindt implementatie plaats van de activiteiten c.q. maatregelen die zijn opgenomen in het beveiligingsplan volgens een daarop afgestemd planningsschema.

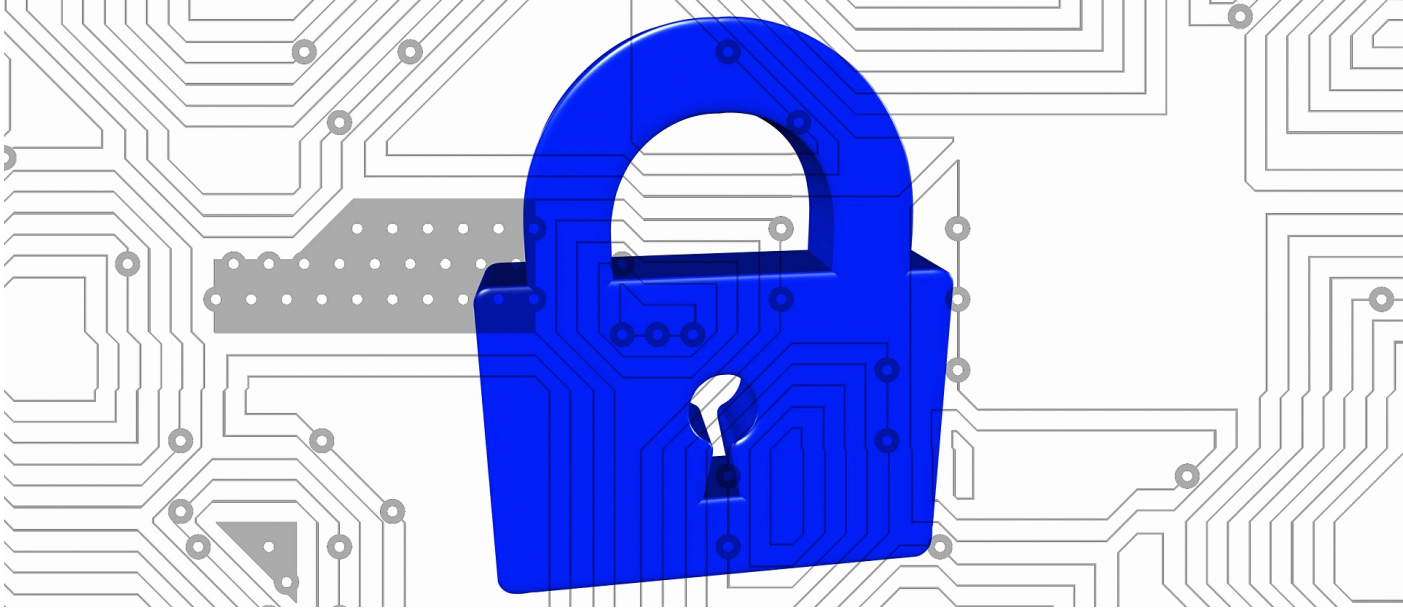
CHECK

In de CHECK-fase vindt periodieke controle plaats op de werking van de vastgestelde beheersmaatregelen. Daarbij kan gedacht worden aan:

- interne controle uitgevoerd door concern control met gebruikmaking van het tactisch toetsingskader van de BIG (zie hoofdstuk 4);
- zelfevaluaties op de BRP en reisdocumenten (Burgerzaken);
- externe controle op DigiD, SUWI, BAG en BRP en PUN;
- testen van de werking zoals de naleving van een clear desk policy (opgeruimde werkplekken en kopieerplekken), beoordelen van loggings op afwijkende patronen, het uitvoeren van penetratietesten om kwetsbaarheden in het netwerk te detecteren, het testen van de backup & recovery procedure of het testen van continuiteits- c.q. uitwijkplannen;
- Beoordelen van beveiligingsincidenten.

ACT

In de ACT-fase vindt evaluatie plaats aan de hand van de bevindingen uit de CHECK-fase. Tussentijds vindt voortgangsrapportage plaats die aansluit op de P&C cyclus van de gemeente. Gesignaleerde verbeterpunten komen terug in de PLAN-fase voor het nieuwe jaar in de vorm van een geactualiseerd informatiebeveiligingsplan waarmee de start van een nieuwe PDCA-cyclus begint.



Het beleid van de gemeente Velsen is gebaseerd op de Baseline Informatiebeveiliging voor Gemeenten (BIG) en deze bestaat uit 2 delen, te weten een strategisch en tactisch deel[10].

De Strategische Baseline kan gezien worden als een 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. Dit deel vinden we terug in het ISMS dat vanuit een PDCA-cyclus grip houdt op het proces.

De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor de gemeenten. Het is feitelijk het toetsingskader waaraan inhoudelijk moet worden voldaan. De Tactische Baseline hanteert de volgende indeling:

- Beveiligingsbeleid
- Organisatie van informatiebeveiliging
- Beheer van bedrijfsmiddelen
- Beveiliging van personeel
- Fysieke beveiliging
- Beheer van communicatie- en bedieningsprocessen
- Toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- Beheer van incidenten
- Bedrijfscontinuïteit
- Naleving

De hierin opgenomen maatregelen behoren te worden geïmplementeerd vanuit een risicobenadering en vanuit het principe 'pas toe of leg uit'. Dat wil zeggen, dat elke control moet zijn geïmplementeerd tenzij er motiverende redenen zijn om daarvan af te wijken.

Het implementeren, verdiepen en onderhouden van de baseline binnen de gemeente Velsen is een groeiproces wat zeker enkele jaren in beslag zal nemen om op het gewenste beveiligingsniveau volgens de BIG te komen. Dat heeft onder meer te maken met beschikbare capaciteit, leermomenten en met een cultuuromslag in het denken en handelen rond dit thema wat doorgaans een geleidelijk proces is.

De eisen ten aanzien van de eerste 2 onderwerpen uit de BIG, te weten beveiligingsbeleid en organisatie van de informatiebeveiliging zijn al in voldoende mate

[10] Beide documenten zijn te downloaden via https://www.kinggemeenten.nl/

behandeld in dit beleidsdocument. Voor de overige onderwerpen uit de BIG gelden op hoofdlijnen de volgende eisen[11].

4.1 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. Op basis van dat inzicht kunnen bedrijfsmiddelen geclassificeerd worden en is de organisatie beter in staat om verantwoorde keuzes te maken ten aanzien van het niveau van beveiligen.

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 groen gemarkeerde deel is afgedekt door de BIG. Voor kritische informatie die daarbuiten valt, zijn aanvullende beveiligingsmaatregelen nodig. Deze komen in beeld aan de hand van een gedegen risicoanalyse. Het streven is om een zo laag mogelijk classificatieniveau te bepalen om onnodige beveiligingskosten te voorkomen.

[11] De werkelijke stand van zaken en nog uit te voeren verbeteractiviteiten zijn terug te vinden in het informatiebeveiligingsplan van de gemeente Velsen.

Het object van classificatie is informatie en classificatie vindt plaats op het niveau van informatiesystemen. De eigenaar van de gegevens bepaalt het niveau van classificatie en houdt daarbij eveneens rekening met wettelijke eisen.

4.2 Beveiliging van personeel

De beveiliging van personeel is een van de belangrijkste aandachtsgebieden vanwege het gegeven dat de meeste beveiligingsincidenten 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 beveiliging van personeel is onderscheid in een 3-tal deelgebieden, te weten voorafgaand aan het dienstverband[12], tijdens het dienstverband en beëindiging of wijziging van het dienstverband.

Voorafgaand aan het dienstverband gaat het om het bewerkstelligen dat de betrokkenen hun verantwoordelijkheden begrijpen en geschikt zijn voor de overwogen rollen en om het verminderen van het risico op diefstal, fraude of misbruik van faciliteiten.

Tijdens het dienstverband ligt de nadruk op het bewerkstelligen dat betrokkenen zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheden en aansprakelijkheden en dat zij zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen.

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.

4.3 Fysieke beveiliging

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).

4.4 Beheer van communicatie- en bedieningsprocessen

Het beheer van communicatie- en bedieningsprocessen is gericht op het handhaven van de noodzakelijke beveiligingseisen op het beheer en gebruik van ICT-voorzieningen binnen de gemeente. Belangrijke aandachtsgebieden zijn:

- borging van het beheer van de ICT-voorzieningen zowel intern (ICT-afdeling) als extern (bij uitbesteding) om zoveel mogelijk fouten, storingen, uitval en problemen rondom de continuïteit te voorkomen. Het gaat hier voornamelijk op het naleven van ICT-beheerprocedures;

[12] Dienstverband is in dit kader een ruim begrip. Hiermee wordt onder meer bedoeld tewerkstelling van personen (tijdelijk of langer verband), benoeming in functies, wisseling van functies, toewijzing van contracten en de beëindiging van enige van deze overeenkomsten.

- capaciteitbeheer en systeemacceptatie om het risico van systeemstoringen tot een minimum te beperken;
- bescherming van de integriteit van programmatuur en informatie tegen virussen en ongeautoriseerde 'mobile' code[13];
- een goed werkende procedure voor backup en recovery om de integriteit en beschikbaarheid van informatie en IT-voorzieningen te handhaven;
- borging van het beheer van het netwerk om de informatie in het netwerk en de onderliggende IT-infrastructuur te beschermen;
- bescherming van verwijderbare opslagmedia tegen ongeautoriseerd gebruik om openbaarmaking, modificatie, verwijdering of vernietiging te voorkomen;
- beveiligd uitwisselen van informatie binnen de organisatie en aan derden (denk aan koppelingen systemen, maar ook aan e-mail en gebruik van social media);
- beveiligde digitale dienstverlening van de gemeente ter bescherming van informatie (integriteit, vertrouwelijkheid en beschikbaarheid);
- controle op de logging van gebruikers en beheerders van ICT-voorzieningen om onbevoegde informatieverwerkingsactiviteiten te ontdekken.

4.5 Logische toegangsbeveiliging

Logische toegangsbeveiliging is het geheel aan maatregelen met als doel de toegang tot gegevens en informatiesystemen te beheersen, zodat gegevens, informatiesystemen en resources 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;
- het naleven van een clear desk- en clear screen beleid, ofwel ervoor zorgdragen dat elke werkplek na werktijd is opgeruimd (gevoelige en bedrijfskritische informatie op papier en verwijderbare opslagmedia), dat computerapparatuur is uitgeschakeld en dat sprake is van schermbeveiliging bij het tijdelijk verlaten van de werkplek;
- 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.

[13] Mobile code bestaat uit kleine programmaatjes die tussen systemen onderling worden uitgewisseld en is nodig om een systeem goed te laten werken.

4.6 Verwerving, 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;
- het voorzien van adequate beheersmaatregelen in informatiesystemen waaronder de validatie op invoergegevens, interne verwerking en uitvoergegevens;
- het definiëren van beleid over de noodzaak van het gebruik van cryptografie (versleutelen van gegevens) voor de bescherming van gevoelige informatie[14];
- 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;
- procedures om tijdig te kunnen reageren op technische kwetsbaarheden die zijn gesignaleerd, hetzij intern dan wel via externe bronnen zoals de IBD of leveranciers van ICT-voorzieningen.

4.7 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.

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. Alle medewerkers en externe gebruikers zijn op de hoogte van deze procedure.

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

4.8 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 kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en op het bewerkstelligen van tijdig herstel.

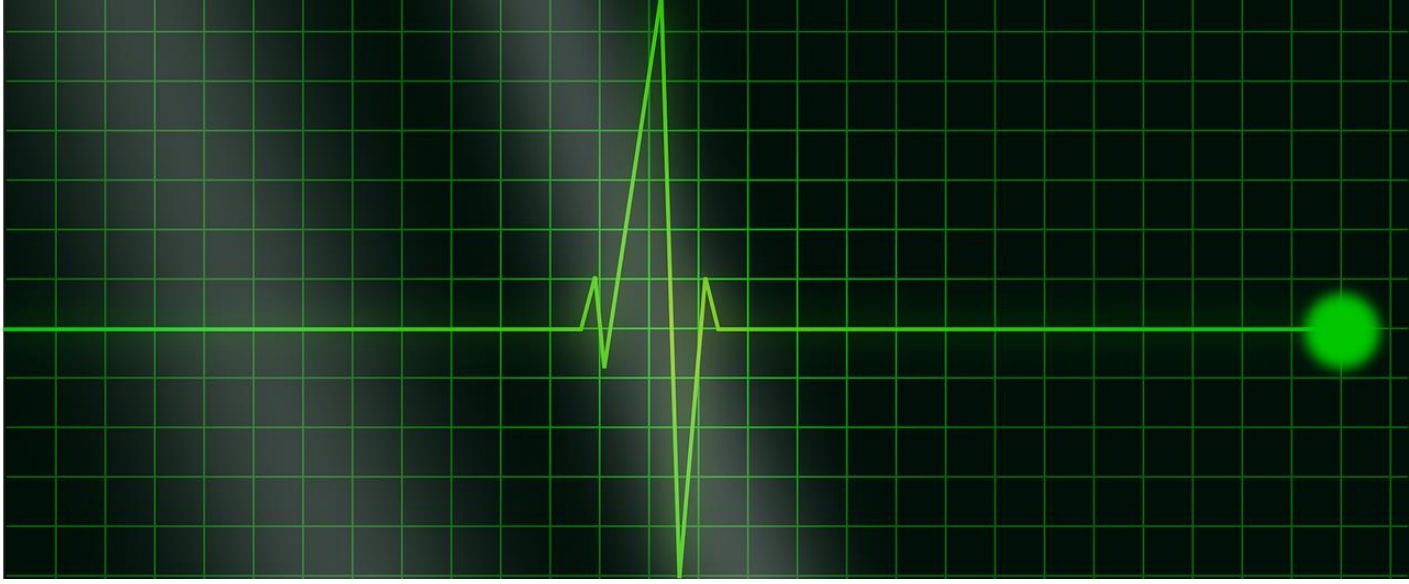
[14] Dit is beleid op het niveau van de bedrijfsvoering.

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

4.9 Naleving

In dit onderdeel ligt de nadruk om 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 privacy wetgeving Wbp die heel nadrukkelijk in beeld komt in het sociaal domein (drie decentralisaties).

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.



5.1 Scope

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit gemeentelijke IB-beleid is een algemene basis. Voor bepaalde kritische processen gelden specifieke (aanvullende) beveiligingseisen.

5.2 Kritische processen

Met de BIG wordt er aan een basisniveau van beveiliging voldaan. Of dit voor alle gemeentelijke processen voldoende is moet worden bepaald door de meest belangrijke processen apart te beschouwen. Voor deze kritische processen wordt dan onderzocht of de BIG voldoende bescherming biedt (baselinetoets). Als dit niet het geval is volgt de uitvoering van risicoanalyses zodat aanvullende beveiligingsmaatregelen worden genomen.

Wat zijn dan die kritische processen? Om dat te kunnen bepalen wordt er naar een aantal criteria gekeken:

- 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.

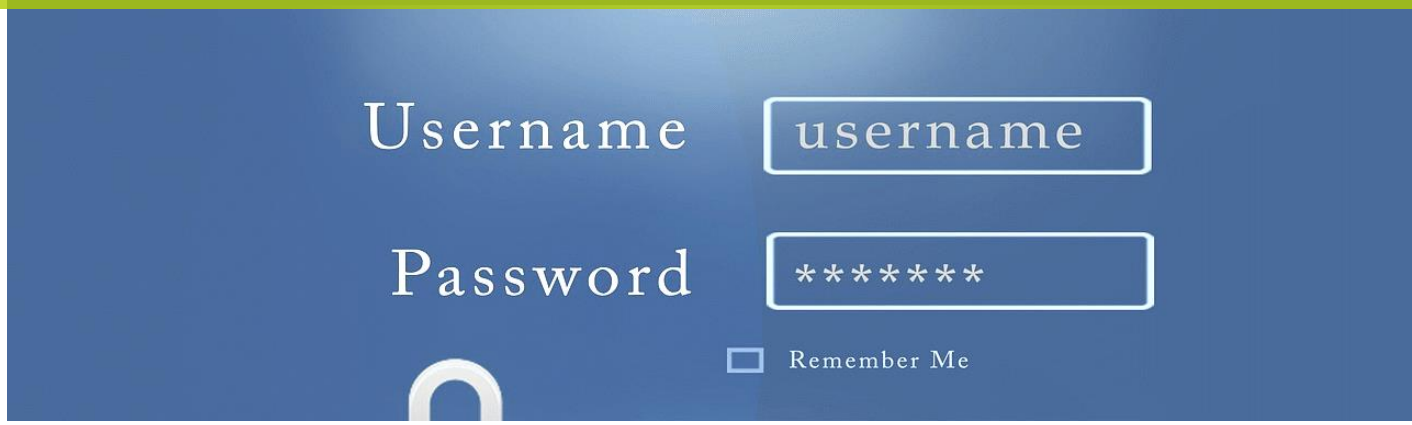
Op basis van deze criteria zijn bij de gemeente Velsen de volgende kritische processen geïdentificeerd:

- Basisregistraties
- Belastingen
- Dienstverlening Burgerzaken
- Dienstverlening Sociaal Domein (met speciale aandacht voor Suwinet)
- Financiële administratie
- Openbare orde en veiligheid
- Vergunningverlening
- Beheer personeelszaken

De eigenaar van het proces[15] voert een toets uit waarmee wordt bepaald of de BIG voldoende beveiliging biedt. Wanneer blijkt dat dit onvoldoende is wordt er een risicoanalyse uitgevoerd waarbij alle betrokken digitale en analoge systemen worden meegenomen. De CIB levert ondersteuning bij de toets en de risicoanalyse.

[15] Nog te bepalen, veelal zal dit een afdelingsmanager of teamleider zijn.

6. Toegang tot informatie



Een belangrijke oorzaak van het ontstaan van beveiligingslekken is de manier waarop medewerkers reageren op een onvolledige informatievoorziening. Wanneer medewerkers geen toegang hebben tot informatie die ze nodig hebben voor de uitoefening van hun werkzaamheden gaan ze 'op zoek' naar die informatie. In de praktijk betekent dat vaak dat er wachtwoorden en inlogcodes worden 'geleend' van collega's.

Naast maatregelen die de toegang tot informatie beperken zijn er dus ook maatregelen nodig die juist zorgen voor toegang tot informatie. Het is belangrijk dat medewerkers toegang krijgen tot alle informatie die ze voor het uitvoeren van hun werkzaamheden nodig hebben. Het is daarom van belang dat er ook aandacht wordt besteed aan het in kaart brengen van de informatiebehoefte en het ontsluiten van relevante informatie voor de medewerkers die deze informatie nodig hebben.

Door zo veel mogelijk informatie op maat te ontsluiten met behulp van softwareapplicaties die primair gericht zijn op het raadplegen van informatie, wordt het eenvoudiger om binnen de wettelijke kaders te opereren. Daarnaast zal de informatie voor medewerkers toegankelijker zijn waardoor ze over betrouwbare gegevens kunnen beschikken en geen eigen (schaduw) administraties meer bij hoeven te houden. Het bijhouden van dubbele administraties is inefficiënt en verhoogt het risico op het werken met incorrecte gegevens.

Deze beleidsnota vormt, samen met het nog op te stellen informatiebeveiligingsplan, het fundament onder een betrouwbare informatievoorziening. Het informatiebeveiligingsplan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen en registraties in het incidentenregister.

De informatievoorziening is een aspect van de bedrijfsvoering, de verantwoordelijkheid voor betrouwbaarheid van de informatievoorziening valt daarom onder de gemeentesecretaris.

De gemeentesecretaris legt de verantwoordelijkheid voor het opstellen van een informatiebeveiligingsplan en voor de procesmatige bewaking van de uitvoering van dit plan neer bij afdelingsmanager Informatiemanagement. Het informatiebeveiligingsplan wordt gebaseerd op dit beleid, het BIG-normenkader, externe ontwikkelingen, een risicoanalyse en geregistreerde incidenten. De daaruit voortvloeiende maatregelen worden geïmplementeerd in de organisatie, bewaakt en periodiek (jaarlijks) geëvalueerd. De afdelingsmanager Informatiemanagement zal deze taken delegeren aan de coördinator informatiebeveiliging.

De gemeentesecretaris legt de verantwoordelijkheid van de implementatie van de genoemde maatregelen neer bij de afdelingshoofden die daarbij worden aangestuurd door de Afdelingsmanager Informatiemanagement.

Door de implementatie, het bewaken en de periodieke evaluatie van de beveiligingsmaatregelen zal de betrouwbaarheid van de informatievoorziening worden verhoogd en de kwaliteit van de informatievoorziening worden gewaarborgd. De coördinator informatiebeveiliging ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover. Informatiebeveiliging is een van de kwaliteitscriteria waarover in de P&C cyclus wordt gerapporteerd. Het aspect informatiebeveiliging wordt als paragraaf opgenomen binnen het onderdeel informatiemanagement in de P&C cyclus.

Daarnaast is het van belang om in te toekomst de informatiebeveiliging gezamenlijk met samenwerkingspartners te organiseren. Daarbij is het goed om vast te stellen dat verschillen in de eisen aan informatiebeveiliging samenwerking onnodig complex kan maken en dat er genoeg tijd genomen moet worden om geleidelijk naar elkaar toe te groeien.