Gemeente Zeist

Bijlage 1.

Beleid Informatieveiligheid 2016 – 2018

Weerbaar en Bewust

Documentcode:	Bijlage bij Collegevoorstel: 16CV00317
Versie:	1.0 (16cv.0037)
Versiedatum	13 september 2016
Gemaakt door:	D. van de Guchte & A. van Leeuwen
Goedgekeurd door:	College van B&W
V-Classificatie:	Intern document / openbaar

Gemeente Zeist

Versiegegevens

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
10-12-2015	0.1	Key2control	Basisdocument
19-04-2015	0.2	D. van de Guchte	Op Zeist afgestemd
16-09-2016	0.3	D. van de Guchte & A. van Leeuwen	Organisatiestructuur

Inhoudsopgave

1. Inleiding en samenvatting

1.1. Inleiding

Voor u ligt het **Beleid Informatieveiligheid 2016 - 2018 Weerbaar en Bewust** van gemeente Zeist waarin onder meer de kaders, uitgangspunten, verantwoordelijkheden en richting om informatiebeveiliging structureel te borgen in de gemeentelijke organisatie zijn vastgelegd. De CISO[1] heeft dit document opgesteld samen met een team bestaande uit security gerelateerde functionarissen van de gemeente.

Het belang van informatieveiligheid
Informatiebeveiliging is geen doel op zich, maar moet de primaire bedrijfsprocessen ondersteunen en de veilige en verantwoorde uitvoering daarvan mogelijk maken. Informatiebeveiliging dient vanuit het primaire proces gestuurd te worden, daar waar het eigenaarschap van de informatie ligt. Informatiebeveiliging is erop gericht vertrouwelijke informatie afdoende te beschermen tegen misbruik of ongeautoriseerde toegang, maar ook om de beschikbaarheid en integriteit van de informatie en daaraan verbonden dienstverlening te blijven garanderen. Een overheid die informatieveiligheid niet omarmt, verliest het vertrouwen van de burger en daarmee haar legitimiteit.

Niet voor niets heeft de VNG eind 2013 het belang van informatiebeveiliging benadrukt door in een algemene ledenvergadering een resolutie te bekrachtigen waarin staat dat informatieveiligheid wordt opgenomen in de portefeuille van een van de leden van het college van B&W en dat de Baseline Informatiebeveiliging Gemeenten (BIG) het gemeentelijke basisnormenkader voor informatieveiligheid wordt. In deze resolutie is ook aangegeven dat gemeenten de informatie-veiligheid zowel bestuurlijk als organisatorisch borgen en deze transparant maken voor burgers, bedrijven en (keten)partners.

Een andere ontwikkeling waarin het belang van informatiebeveiliging tot uiting komt, is vanuit de Wet bescherming persoonsgegevens (Wbp). In artikel 13 Wbp is opgenomen dat de verantwoordelijke (lees het college van B&W) passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Sowieso is deze wet van toepassing op gemeenten, maar begin 2016 is daaraan toegevoegd de Meldplicht datalekken (lekken van persoonsgegevens) en krijgt het CBP[2] meer boetebevoegdheid tot € 810k per overtreding. Het niet voldoen aan de Wbp kan leiden tot aanzienlijke reputatieschade en extra kosten als gevolg van opgelegde boetes en herstelwerkzaamheden.
Het mag duidelijk zijn dat informatiebeveiliging en het beschermen van persoonsgegevens onlosmakelijk met elkaar zijn verbonden. Onvoldoende of gebrekkige informatiebeveiliging kan aldus nadelig uitvallen vanuit de bescherming van persoonsgegevens (Wbp).

Reden te meer om informatiebeveiliging structureel te borgen in de organisatie. Dit beleidsdocument is normstellend en biedt daarvoor de basis. Centraal ligt de nadruk op het realiseren van een ISMS wat staat voor een Information Security Management System ofwel een informatie beveiligingsmanagementsysteem. Een ISMS is als het ware de 'motor' die zorgdraagt voor de periodieke planning, implementatie, onderhoud, beoordeling en het verder verbeteren van de informatiebeveiliging binnen de context van de gemeente.

[1] CISO staat voor Chief Information Security Officer
[2] CBP staat voor College Bescherming Persoonsgegevens en heet vanaf 2016 Autoriteit Persoonsgegevens

Met een ISMS is de gemeente beter in staat om informatiebeveiliging te managen, bedrijfsmiddelen te beschermen, de bewustwording en acceptatie van informatiebeveiliging bij medewerkers te versterken, ongeautoriseerde toegang tot informatie te voorkomen, snel en adequaat te kunnen reageren op beveiligingsincidenten, persoonsgegevens van burgers en medewerkers te beschermen, de bedrijfscontinuïteit te garanderen en te voldoen aan naleving van wet- en regelgeving.

1.2. Samenvatting

Het college van B&W en het management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Het college van B&W geeft een duidelijke richting aan informatie-beveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt door het vaststellen en uitbrengen van informatiebeveiligingsbeleid voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). De uitwerking van dit beleid naar de organisatie ligt bij het management. Het management stuurt op risico's, bepaalt welke beveiligingsmaatregelen nodig zijn, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Het management wordt hierbij ondersteund door de CISO.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt dat:

- er wetgeving is waar altijd aan voldaan moet worden, zoals niet uitputtend de BRP[3], PUN, SUWI en BAG, maar ook de archiefwet, Wet bescherming persoonsgegevens (Wbp), de Wet openbaarheid van bestuur (Wob) en de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG);
- een gemeenschappelijk normenkader voor informatiebeveiliging als basis dient, te weten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
- de gemeente dit normenkader vaststelt waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

[3] BRP staat voor Basisregistratie Personen, PUN staat voor Paspoort uitvoeringsregeling Nederland, SUWI staat voor Wet structuur uitvoeringsorganisatie werk en inkomen en BAG staat voor Basisregistratie adressen en gebouwen.

De gemeente hanteert de volgende uitgangspunten:

1. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het College van B&W als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.

2. 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 organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

3. Informatiebeveiliging is een continu leer- en verbeterproces. Het ISMS bestaande uit een plan-do-check-act cyclus is het managementsysteem van informatiebeveiliging en bedoeld voor alle actoren die vanuit de governance een sturende, coördinerende, uitvoerende en controlerende functie hebben om grip te blijven houden op de kwaliteit van de informatiebeveiliging.

4. De CISO[4] ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de informatieveiligheid en rapporteert hierover aan het management. De CISO is eveneens het centrale aanspreekpunt voor informatiebeveiliging.

5. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

6. Regels en verantwoordelijkheden voor het beveiligingsbeleid worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.

7. 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.

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

4 CISO staat voor Chief Information Security Officer

2. Informatiebeveiliging

2.1. Visie op informatiebeveiliging en privacy

De komende jaren zet gemeente Zeist 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. Dit vereist een integrale aanpak, open en transparant, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Een integraal onderdeel van de Informatieveiligheid is de privacy. Een bestaand iets, maar in de afgelopen jaren, mede door de digitalisering en brede uitwisseling (ketensamenwerking) van informatie, veel actueler geworden. Het raakt de persoonlijke levenssfeer en vereist een andere houding en invulling van de overheid. Want gemeenten zijn niet alleen verantwoordelijk voor het borgen van de privacy van hun inwoners, maar ook deels voor het zorgvuldig omgaan met persoonsgegevens in de ketens die zij regisseren en de netwerken waarin ze samenwerken. Vanuit dit oogpunt is het noodzakelijk een visie op privacy te formuleren. Zodat deze gebruikt kan worden als kapstok om de diverse uitvoeringszaken, zoals bijvoorbeeld de regie op eigen gegevens, vorm te geven.

De visie luidt als volgt:
Privacy en de kunst van het selectief verzamelen. De balans tussen afstand en nabijheid.
Door precies die beperkte hoeveelheid informatie te verzamelen en te gebruiken die nodig is voor de taakuitoefening en dit steeds te toetsen, zijn we als overheid een betrouwbare partner. Door niet uit te gaan van risicomijding, maar professionaliteit, werken we vanuit ieders kracht.

2.2. Definitie van informatiebeveiliging

Informatiebeveiliging is het samenhangend stelsel[5] van beheersingsmaatregelen dat de beschikbaarheid/continuïteit, de integriteit/betrouwbaarheid en exclusiviteit/ 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 / continuïteit: zorgen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- integriteit / betrouwbaarheid: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- exclusiviteit / vertrouwelijkheid: beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

[5] Met een samenhangend stelsel wordt bedoeld dat de verschillende maatregelen die samen de informatiebeveiliging vormen niet van elkaar los worden getroffen, maar in onderlinge relatie met elkaar staan.

2.3. Doel beleid en doelgroep

Dit informatiebeveiligingsbeleid is het kader voor passende bestuurlijke, technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving en het vertrouwen van haar klanten waardig is. Gemeente Zeist 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 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).

Het college van B&W, managementteam en lijnmanagement dragen de inhoud uit naar alle medewerkers en gebruikers die zijn betrokken bij de verwerking en beheer van informatie en/of het beheer van informatiesystemen, waarvan de verantwoordelijkheid bij de gemeente Zeist ligt. Het informatiebeveiligingsbeleid is van toepassing voor alle medewerkers en gebruikers van informatie.

2.4. 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, 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 enz.) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar vooral ook mensen en processen.

2.5. Grondslagen

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

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, niet uitputtend, de Basisregistratie personen (BRP), Paspoort uitvoeringsregeling Nederland (PUN), de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), de Basisregistratie adressen en gebouwen (BAG), de archiefwet, de Wet bescherming persoonsgegevens (Wbp) en de Wet openbaarheid van bestuur (Wob). 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.

Dit beleid dekt overigens de Wbp niet geheel af. Daarvoor is als basis privacy beleid nodig dat verder uitgewerkt moet worden in concrete governance, procedures, maatregelen en richtlijnen. Informatiebeveiliging heeft uiteraard wel raakvlakken, maar is slechts een van de randvoorwaarden om überhaupt te kunnen voldoen aan de eisen van de Wbp.

2.6. Uitgangspunten

Gemeente Zeist hanteert de volgende uitgangspunten:

1. Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor een efficiënte en effectieve bedrijfsvoering. Omdat de gemeente Zeist onderdeel uitmaakt van de totale overheid en ook verbonden is met andere ketenpartijen, heeft een onveilige situatie bij de gemeente Zeist direct gevolgen voor de veiligheid van andere overheden of partijen.

2. Informatiebeveiliging is noodzakelijk om de betrouwbaarheid, integriteit en continuïteit van de informatievoorziening te kunnen borgen.

3. De informatiebeveiligingstaken worden als integraal onderdeel van de dagelijkse bedrijfsvoering in de organisatie belegd.

4. Informatiebeveiliging is niet vanzelfsprekend en moet georganiseerd worden. Het vergroten van het bewustzijn en acceptatie van medewerkers over informatiebeveiliging vraagt continue aandacht van het management.

5. 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, is actualisering van het informatiebeveiligingsbeleid minimaal om de 3 jaar nodig of eerder indien zich belangrijke wijzigingen voordoen. Hiervoor vinden periodiek risicoanalyses plaats en om de controle en de kwaliteit van de informatieveiligheid te waarborgen wordt informatiebeveiliging in de P&C cyclus van de gemeente opgenomen.

6. Periodiek onafhankelijke controle is nodig om vast te stellen of de informatiebeveiliging voldoet aan het informatiebeveiligingsbeleid en of de uitgevoerde maatregelen voldoende zijn om het gewenste niveau van informatiebeveiliging te bewerkstelligen.

7. Informatiebeveiliging moet bij voorkeur informatiebeveiligingsincidenten voorkomen, respectievelijk de effecten van het optreden van incidenten beperken.

8. Informatiebeveiligingsmaatregelen mogen niet ten koste gaan van de veiligheid van eigen personeel en van derden en dienen zo min mogelijk ten koste te gaan van andere sturingsprincipes van de gemeente Zeist zoals flexibiliteit en klantgerichtheid (spanningsveld).

9. 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.

10. 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 aan de leidinggevenden of de beveiligingsmedewerkers. Gemeente Zeist 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.

11. Personen krijgen niet meer autorisaties dan nodig voor het uitvoeren van hun taken.

2.7. Risicobenadering

Gemeente Zeist volgt een aanpak van informatiebeveiliging op basis van risicobeheersing. Het streven naar 100% beveiliging heeft geen zin, is een utopie en zou te belastend zijn voor de organisatie. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van beveiligingsmaatregelen te implementeren en om daarbij een betere afweging tussen kosten en noodzaak te maken.

Het startpunt voor een gestructureerde opbouw is het uitvoeren van een nulmeting op basis van de BIG en bedoeld om inzicht te krijgen in het zogenaamde ‘gat’ tussen datgene wat nodig is en wat ontbreekt. Op basis van dat inzicht vindt een impactanalyse plaats waardoor de gemeente in staat is om prioritering te geven aan verbeterpunten voor de korte (denk aan quick wins) en lange termijn. Bij deze benadering is ruimte voor afweging en prioritering op basis van het principe ‘pas toe of leg uit’.

Indien een gemeentelijk proces meer beheersingsmaatregelen nodig heeft dan vindt hierop een (uitgebreide) risicoanalyse plaats. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van het werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident.

2.8. Samenwerking

Intergemeentelijke samenwerking en het samenwerken met ketenpartners heeft er al toe geleid dat er steeds vaker en andere informatie wordt uitgewisseld met samenwerkingspartners. De ontwikkelingen in het sociaal domein zijn hiervan een sprekend voorbeeld. Met samenwerkingspartners waar informatiebeveiliging een rol speelt worden afspraken gemaakt over het vereiste niveau van informatiebeveiliging die de gemeente Zeist stelt. In sommige gevallen kan dit hoger liggen dan de vereisten volgens de BIG. Denk in dat geval aan privacy gevoelige gegevens.

3. Organisatie van de informatiebeveiliging

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 gemaakt over de daarbij behorende verantwoordelijkheden, taken en rollen. Het gaat hier over de governance rond informatiebeveiliging waarbij onderlinge samenwerking en afstemming - en ieder vanuit zijn eigen verantwoordelijkheid - bepalend is voor het succes van een goed werkend ISMS.

3.2. Verantwoordelijkheden

Het college van B&W is bestuurlijk verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente en stelt kaders op voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

De Informatiemanager, het hoofd van de afdeling Informatie Voorziening is ambtelijk verantwoordelijk voor de beveiliging van informatie en de daarbij behorende algemene sturing.

Het team informatieveiligheid en privacy:

- 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 waar nodig bij.

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

- 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 bewustzijn);
- meldt incidenten en rapporteert in hoeverre hun organisatieonderdeel compliance is aan het informatiebeveiligingsbeleid van de gemeente.

En is verantwoordelijk voor de uitvoering van:

- de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyse.
- alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegenheden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, logging van activiteiten en back-up & recovery;
- maatregelen gericht op beveiliging van personeel zoals screening, geheimhoudingsverklaringen en awareness programma's;
- maatregelen gericht op beveiliging van gebouwen, publieke en werkruimte van de gemeente;

- activiteiten die gericht zijn op het inrichten 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 het hoofd van de afdeling Informatie Voorziening en informeert de raad over dit thema. Binnen het college van B&W valt informatiebeveiliging onder de portefeuille van de wethouder Informatievoorziening. Het Team Informatieveiligheid en Privacy adviseert het college van B&W formeel over het vast te stellen beleid.

Het Informatiemanager geeft sturing aan de uitvoering van het informatiebeveiligings-beleid en ziet erop toe dat naleving van dit beleid plaatsvindt. De taken die hieruit voortvloeien zijn belegd bij de CISO en haar Team informatieveiligheid en Privacy. De CISO bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert jaarlijks concernbreed aan het College van B&W over de stand van zaken.

De CISO heeft een adviserende faciliterende en coördinerende rol en zorgt ervoor dat uitvoerende taken zoveel mogelijk belegd zijn bij het lijnmanagement. Controlerende taken op het gebied van informatie-beveiliging liggen zoveel mogelijk bij de afdeling concern control. Een functieprofiel van de CISO is uitgewerkt.

Alle organisatieonderdelen hebben minimaal 1 aanspreekpunt voor de CISO. Periodiek voert de CISO overleg met deze contactpersonen en eventueel andere security gerelateerde medewerkers (denk aan privacy gerelateerde activiteiten) over de stand van zaken en nieuwe ontwikkelingen op het gebied van informatiebeveiliging. De resultaten hiervan neemt de CISO mee in zijn evaluatie

3.4. ISMS

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

4. Baseline Informatiebeveiliging Gemeenten (BIG)

4.1. Inleiding

Zoals in paragraaf 2.5 is aangegeven, is het informatiebeveiligingsbeleid van de gemeente gebaseerd op de BIG versie 1.01. Documentatie hierover is standaard beschikbaar via de Informatie-beveiligingsdienst voor gemeenten (IBD)[6]. De gemeente heeft zich aangesloten op de dienstverlening van de IBD en bij de uitwerking van dit beleid zal zoveel mogelijk gebruik gemaakt worden van reeds beschikbare documentatie / handreikingen van de IBD.

De BIG bestaat uit 2 delen, te weten een strategisch en tactisch deel en is gebaseerd op een internationale standaard en wel de NEN/ISO 27001: 2005 voor het strategische deel en NEN/ISO/27002: 2007 voor het tactische deel. De Strategische Baseline is feitelijk de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen worden en is sterk gericht op de governance van informatiebeveiliging. De organisatie en de verantwoording over informatie-beveiliging staat hierin centraal.

De Tactische Baseline beschrijft de normen en beveiligingsmaatregelen die een samenhangend stelsel van beveiligingsmaatregelen vormen. Aan de hand van een risicoanalyse wordt bepaald welke maatregelen ingezet worden en in welke mate volgens het principe 'pas toe of leg uit'. Deze maatregelen behoren vervolgens te worden geïmplementeerd en periodiek te worden getoetst op naleving en effectiviteit.

Het implementeren, verdiepen en onderhouden van de baseline binnen de gemeente Zeist is een leer- en groeiproces wat zeker enkele jaren in beslag zal nemen om op het gewenste beveiligingsniveau volgens de BIG te komen. Het is vooral de menselijke factor die hierbij een belangrijke rol speelt en uit dien hoofde is veel aandacht nodig voor het versterken van de bewustwording en acceptatie bij alle medewerkers. Een gemeente kan nog zoveel technische beveiligingsmaatregelen nemen, wanneer medewerkers er niet naar handelen hebben deze maatregelen uiteindelijk aanzienlijk minder effect.

De Tactische Baseline hanteert de volgende indeling:

- H5: Beveiligingsbeleid
- H6: Organisatie van informatiebeveiliging
- H7: Beheer van bedrijfsmiddelen
- H8: Beveiliging van personeel
- H9: Fysieke beveiliging
- H10: Beheer van communicatie- en bedieningsprocessen
- H11: Logische toegangsbeveiliging
- H12: Verwerving, ontwikkeling en onderhoud van informatiesystemen
- H13: Beheer van incidenten
- H14: Bedrijfscontinuïteit
- H15: Naleving

[6] Zie www.ibdgemeenten.nl/downloads/

De hoofstukken verwijzen naar de indeling uit de tactische BIG. De items in H5 en H6 zijn al uitvoerig behandeld in dit beleidsdocument. In de volgende paragrafen wordt nader ingegaan op belangrijke items in H7 t/m H15.

4.2. Beheer van de bedrijfsmiddelen

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen en dienen te worden beschermd. Deze middelen kunnen immers blootgesteld zijn aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik. Van belang is dat alle relevante bedrijfsmiddelen bekend zijn, voorzien zijn van een eigenaar/hoofdgebruiker en voorzien zijn van geschikte beveiligingsmaatregelen. De procedures configuratiebeheer, dataclassificatie en de baselinetoets ondersteunen de organisatie om grip te houden op het beheer van bedrijfsmiddelen.

Informatie kan meer of minder gevoelig of kritisch zijn en voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Voor dataclassificatie is de volgende tabel in het kader van de BIG van toepassing:

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

Het gemarkeerde deel is afgedekt door de BIG. Voor kritische informatie die daarbuiten vallen, 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.

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.

4.3. 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 , tijdens het dienstverband en beëindiging of wijziging van het dienstverband.

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

Tijdens het dienstverband ligt de nadruk om te 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 te bewerkstelligen dat betrokkenen de organisatie ordelijk verlaten dan wel dat wijziging van het dienstverband ordelijk verloopt.

4.4. Fysieke beveiliging

Fysieke beveiliging is gericht op het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

Aandachtsgebieden zijn de fysieke toegang tot gebouwen, publieke ruimten en werkruimten, maar ook het fysiek afschermen van ICT-voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen (bekabeling, computerruimte, etc).

4.5. 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;
- 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 ;

- een goed werkende procedure voor back-up 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 email en gebruik van social media);
- beveiligde digitale dienstverlening van de gemeente ter bescherming van informatie (integriteit, vertrouwelijk en beschikbaarheid);
- controle op de logging van gebruikers en beheerders van ICT-voorzieningen om onbevoegde informatieverwerkingsactiviteiten te ontdekken.

4.6. 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 definiëren van toegangsbeleid waarin is aangegeven aan welke bedrijfseisen de toegangsbeveiliging moet voldoen en waarbij rekening gehouden wordt met afzonderlijke bedrijfstoepassingen rekening houdend 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) en dat computerapparatuur is uitgeschakeld en 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 hulpprogramma's en programmatuur die toegang geven tot informatie (denk aan query tooling, maar ook snelkoppelingen) tegen onbevoegd gebruik;
- het waarborgen van de informatiebeveiliging bij het gebruik van telewerken en/of mobiele apparatuur.

4.7. Verwerving, ontwikkeling en onderhoud van informatiesystemen

Dit onderdeel gaat vooral 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;
- 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.

4.8. Beheer informatiebeveiligingsincidenten

Het beheer van informatiebeveiligingsincidenten is een belangrijk aandachtsgebied in het kader van informatiebeveiliging en dit belang is alleen maar toegenomen vanwege de meldplicht datalekken vanaf 2016. Een beveiligingsincident kan leiden tot ernstige reputatieschade en extra kosten als gevolg van herstelmaatregelen. Het voorkomen of minimaliseren van incidenten is uiteraard beter zoals het implementeren van de preventieve maatregelen uit de tactische BIG, echter incidenten zijn niet uit te bannen en dus zal de organisatie hierop voorbereid moeten zijn. De essentie is om snel en adequaat te kunnen reageren op beveiligingsincidenten die kunnen escaleren en daarvoor zijn voorbereidende maatregelen nodig zoals het snel kunnen mobiliseren van een security response team, draaiboeken, instructies, checklists en het periodiek uitvoeren van oefeningen om na te gaan of de procedure ‘bullet proof’ is.

Voor alle medewerkers is het belangrijk dat zij in staat zijn beveiligingsincidenten te herkennen en weten hoe zij deze incidenten moeten melden. Dit vereist eveneens de nodige oefeningen en trainingen.

4.9. Continuïteitsbeheer

Bij continuïteitsbeheer gaat het om maatregelen die gericht zijn om langdurige onderbreking van bedrijfsactiviteiten bij de gemeente tegen te gaan en om kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen. Het gaat hier niet alleen om de BRP, waar continuïteitsbeheer een verplicht onderdeel is, maar om een gemeentebrede aanpak.

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

4.10. 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 niet uitputtend de BRP, PUN, BAG, SUWI, Wbp en Wob.

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