gemeente Oosterhout

Beveiligingsbeleid

(informatiebeveiliging en privacy)

Gemeente Oosterhout

Versie beheer:

Versie	Datum	Wijziging	Vastgesteld
1.0	16 juni 2022	Concept ingebracht TOD	
1.1	22 juni 2022	Afstemming directie	
1.2		Vaststelling college	

Inleiding

We leven in een samenleving waarin informatie door alle technologische ontwikkelingen steeds vaker digitaal wordt vastgelegd en gedeeld. De gemeente werkt veel met waardevolle en privacygevoelige (digitale) informatie. Informatie is nooit 100% veilig, er is altijd risico. Er zijn verschillende invloeden en factoren die de informatieveiligheid kunnen beïnvloeden. Het is dus heel belangrijk om te sturen op een zo veilig mogelijk informatiegebruik binnen onze organisatie en informatie niet zomaar te delen met externe partijen. Informatiebeveiliging en het nemen van beheersmaatregelen om de risico's te beperken zijn daarbij leidend.
De gemeente Oosterhout wil een betrouwbare organisatie zijn voor haar inwoners, bedrijven en medewerkers. Zorgvuldig omgaan met (persoons) gegevens staat bij ons hoog in het vaandel. Voorheen werden (persoons)gegevensbescherming en informatiebeveiliging los van elkaar georganiseerd. Maar er zijn veel raakvlakken tussen beiden; we kunnen gegevens alleen beschermen wanneer informatiebeveiliging op orde is. Daarom werken we vanuit een integraal beveiligingsbeleid. We dragen zorg voor een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening en -bescherming aantoonbaar te waarborgen.
Het integrale beveiligingsbeleid geldt voor alle processen van de gemeente. Ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet tot ICT, maar heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

1. VISIE & STRATEGIE

Visie

Oosterhout is een betrouwbare gemeente waar gegevens en informatie van inwoners, ondernemers, medewerkers, partners en andere betrokkenen veilig, vertrouwelijk en daarmee zorgvuldig worden verwerkt. Privacy wordt te allen tijde beschermd. Door het borgen van beveiliging toont de gemeente haar betrouwbaarheid.

Deze betrouwbaarheid maken we concreet door de volgende uitgangspunten:

- De gemeente leeft wet- en regelgeving na.
- De gemeente levert continuïteit in dienstverlening en bedrijfsvoering.
- De gemeente zorgt voor effectief risicobeheer.
- De gemeente blijft leren en verbetert continu haar processen.
- De gemeente genereert vertrouwen in haar informatieverwerking- en deling.
- De gemeente leidt haar medewerkers op om zorgvuldig met gegevens om te gaan.

Strategie

We verbinden verschillende aandachtsgebieden op het gebied van beveiliging, vanuit één strategische visie. Dit integrale beleid maakt dat we efficiënt en eensluidend jaarplannen kunnen formuleren en verantwoorden. Door dit jaarlijks te doen, blijven we flexibel en kunnen we inspelen op actuele situaties en ontwikkelingen. Het werken in overeenstemming met de geldende wet- en regelgeving (compliance) blijft belangrijk, maar wordt voorzien van een 'blik vooruit'. Het beleid legt meer dan voorheen de nadruk op het uitvoeren van risicoanalyse.
Om de betrouwbare gemeente uit de visie te worden, werken we vanuit een strategie die is geënt op twee pijlers. Zo kiezen we voor een beleid van 'bewust risico nemen' in plaats van 'onbewust risico

lopen’. De strategie wordt ook vormgegeven door onze ambities omtrent de volwassenheidsladder van betrouwbaarheid, zoals deze in vastgesteld door de Vereniging Nederlandse Gemeenten (VNG) voor privacy en de Informatie Beveiligingsdienst (IBD) voor informatiebeveiliging.

Bewust risico nemen

De gemeente Oosterhout hanteert als uitgangspunt voor beveiliging: 'bewust risico nemen', in plaats van 'onbewust risico lopen'. Alles 100% kunnen beveiligen is een illusie. Technologische ontwikkelingen gaan razendsnel. Kennis moet steeds worden vergoot, systemen moeten steeds worden verbeterd en dan nog is ook databeveiliging deels mensenwerk.
Het is daarom beter dat we bewust zijn van de risico’s die we nemen en daar ons beleid op toespitsen. Een beleid dat is gebaseerd op gefundeerde analyses, ingekleurd door de ervaring van mensen, dat sturing geeft aan wát we doen en hóe we het doen. Dat uit zich in een verschuiving van reactief naar preventief beleid. Tot waar zijn de risico’s acceptabel en beheersbaar? We stellen duidelijke risicoanalyses op. Deze zitten verwerkt in het uitvoeren van de Data Protection Impact Assessments (DPIA’s), maar kunnen ook op andere privacy risico’s worden toegepast.

Volwassenheidsladder

In de toekomstvisie van de gemeente wordt gesteld dat zij een betrouwbare en toekomstbestendige gemeente wil zijn. Hiervoor moet het volwassenheidsniveau van de gemeente op minimaal niveau 3 zijn. Op volwassenheidsniveau 3 vinden de werkzaamheden in herhaalbare en beheerste processen plaats, die zijn gebaseerd op een organisatie breed formeel vastgestelde werkwijze. Daarnaast zijn er beveiligingsrollen benoemd en beschreven. De ambitie is om de komende jaren door te groeien naar niveau 4, waarbij de werkzaamheden plaatsvinden terwijl de kwaliteit van de processen wordt gemeten door het verzamelen van duidelijke gegevens over de processen en hun kwaliteit.

In- en externe factoren

Beveiliging is niet alleen vanuit de interne disciplines te sturen. Er zijn diverse factoren die invloed hebben op de strategie en het beleid op het gebied van beveiliging. Een paar voorbeelden:

- Bestuursakkoord en Strategische visie
  Uit het bestuursakkoord ‘De stap vooruit’ en de Strategische visie ‘Oosterhout ontwikkelt’ blijkt dat de gemeente richting de toekomst meer en nauwer samenwerkt met onder meer onderwijs, ondernemers, inwoners en de gemeenteraad. We hebben dus te maken met veel extra gevoelige, waardevolle gegevens. Dat maakt dat we onze privacybescherming en informatiebeveiliging echt op orde moeten hebben. De keuzes die de gemeente maakt op het gebied van beveiliging moeten aansluiten op deze intensievere samenwerking. Daarnaast streeft de gemeente in al haar beleid naar transparantie en zoveel mogelijk integraal, informatie-gestuurd en programmatisch werken.
- Maatschappelijke ontwikkelingen
  Grote maatschappelijke ontwikkelingen kunnen invloed hebben op de strategie en het beleid van de gemeente. Digitalisering bijvoorbeeld, beïnvloedt de manier waarop we onze dienstverlening organiseren. Ook externe ketenpartners moeten in dit soort processen worden meegenomen. Daarnaast moeten gemeentes steeds meer samenwerken, waarbij het belang van de burger altijd voorop moet staan. Zelfs een pandemie zoals Corona kan gevolgen hebben. Mensen zijn sceptisch over waar hun gegevens allemaal terechtkomen en er is wantrouwen

richting de overheid. Ook de Autoriteit Persoonsgegevens (AP) en de IBD zijn gevoelig voor ontwikkelingen in de samenleving en komen soms met (verplichte) richtlijnen.

2. TACTIEK

Kaders en uitgangspunten

Privacy en informatiebeveiliging zijn zo verweven met elkaar dat we binnen de gemeente Oosterhout uitgaan van een integraal beveiligingsbeleid. Een beleid dat staat of valt met bewustwording. Een gemeente kan nog zo veel technische maatregelen nemen, medewerkers moeten er ook naar handelen. En ook externe factoren kunnen invloed hebben op de beveiliging. Het is een discipline die nooit stil staat. Voor zowel informatiebeveiliging als privacy geldt dat de aanpak risico gebaseerd is. De gemeente Oosterhout gebruikt voor het integrale beveiligingsbeleid de volgende uitgangspunten:

1. **Integrale blik op beveiliging**
   Vanwege de nauwe samenhang tussen informatieveiligheid en privacybescherming benaderen we deze integraal in één gezamenlijk beleid.
2. **Beveiliging begint bij organisatiebewustzijn**
   Beveiliging is mensenwerk. Het vraagt in eerste plaats bewustzijn van het belang van beveiliging en de risico's van een eventueel haperende beveiliging. Dit geldt voor alle medewerkers.
3. **Waarborgen van (privacy)rechten van betrokkenen**
   Inwoners moeten hun rechten kunnen uitoefenen. Zoals het recht op inzage en verwijdering van hun gegevens, het recht om bij de overheid bekende en beschikbare gegevens niet opnieuw te hoeven verstrekken en het recht op transparantie in wat de gemeente doet met de persoonsgegevens van inwoners en aan wie de gemeente deze gegevens verder verstrekt.
4. **Er is een actueel overzicht van gegevensverwerkingen**
   Gegevensverwerkingen zijn in kaart gebracht en worden voortdurend geactualiseerd. Er wordt gedocumenteerd welke persoonsgegevens worden verwerkt en met welk doel en grondslag dit gebeurt, waar deze gegevens vandaan komen en met wie ze worden gedeeld.
5. **Bedrijfsmiddelen zijn geïdentificeerd en geclassificeerd**
   Bedrijfsmiddelen zijn noodzakelijk zijn voor een goede dienstverlening en bedrijfsvoering. Ze kunnen geld kosten of een bepaalde waarde vertegenwoordigen, zoals informatie en data, en apparatuur maar ook mensen en hun kennis. Bedrijfsmiddelen hebben een registratie en classificatie nodig voor een goed beveiligingsniveau.
6. **Bedrijfsmiddelen hebben een eigenaar**
   Bij de geïdentificeerde en geclassificeerde bedrijfsmiddelen zijn eigenaren benoemd. Zij zijn bepalend bij het maken van risicoafwegingen.
7. **Er zijn passende technische- en organisatorische maatregelen genomen**
   Er wordt een zorgvuldige afweging gemaakt tussen mogelijke risico's, het effect ervan en de kosten om deze risico's te voorkomen.
8. **We zien toe op het naleven van maatregelen**
   Naast het nemen van maatregelen zien we uiteraard ook toe op het naleven van maatregelen.
9. **Bewust risico nemen in plaats van onbewust risico lopen**
   Dat betekent dat we per bedreiging bepalen wat de kans is dat deze bedreiging optreed en welke impact de bedreiging heeft op de organisatie. Op basis van impact en kans van optreden maken we een afweging of en zo ja, hoe we het risico willen tegengaan.

10. **'Pas toe of leg uit' principe**
    Het belang en veiligheid van inwoners, bedrijven en andere betrokkenen van de gemeente staan voorop. Het maken van een risicoafweging is om deze reden belangrijk bij het nemen van beslissingen op het gebied van beveiliging.
11. **Beveiliging wordt standaard meegenomen bij het ontwerpen en aanpassen van processen**
    Dit principe houdt in dat we standaard al bij het ontwerpen of aanpassen van producten, diensten, processen of andere organisatorische aanpassingen, voor zorgen dat deze voldoen aan de eisen op het gebied van informatiebeveiliging en privacybescherming.
12. **Beveiliging is geïntegreerd in processen**
    Beveiliging is ingebed in de organisatie, een gekend aspect in de organisatie brede manier van werken. Rekening houden met beveiliging is een 'tweede natuur' van medewerkers.
13. **Beveiligingsincidenten en datalekken worden vastgelegd en gemeld**
    Incidenten en datalekken worden te allen tijde vastgelegd en waar nodig gemeld bij de Autoriteit Persoonsgegevens.
14. **Beveiliging bij derden is geborgd**
    De gemeente besteedt de uitvoering van taken en het beheer van systemen op onderdelen uit aan externe partijen. Het borgen van beveiliging is ook hier een standaard gegeven, bijvoorbeeld door Service Level Agreements, verwerkersovereenkomsten, geheimhoudingsverklaringen en certificering.
15. **Transparantie in de persoonsgegevens die wij verwerken**
    Een overzicht van verwerkingen kan via de website worden ingezien. Bij een verzoek tot inzage geeft de gemeente inzicht in de persoonsgegevens die zij verwerkt over betrokkenen.
16. **Fysieke beveiliging is op orde**
    Naast beveiliging langs elektronische weg is beveiliging nodig van gebouwen en ruimten. Het moet voor iedereen duidelijk zijn welke personen, wanneer toegang hebben tot welke ruimten en op welke manier deze toegang wordt geregeld.
17. **Continuïteit in dienstverlening en bedrijfsvoering is gewaarborgd**
    Uitval van 'kritische' bedrijfsprocessen is onacceptabel. In het continuïteitsplan zijn de acties vastgelegd die moeten worden uitgevoerd, nadat een calamiteit is ontstaan.
18. **We ontwikkelen langs de volwassenheidsladder voor beveiliging**
    Het is een wettelijke verplichting en een maatschappelijk plicht, om de juiste maatregelen te nemen binnen de organisatie en in de techniek. Dit wordt uitgedrukt in volwassenheidsniveaus. De beveiligingsvolwassenheid geeft aan hoe volwassen de gemeente Oosterhout in borging van beveiliging is.

Bewuste medewerkers

Een belangrijk speerpunt in het beveiligingsproces is de bevordering van het beveiligingsbewustzijn bij de medewerkers. Met dit bewustzijn creëren we gedrag. En met dat gedrag wordt het risico dat de gemeente loopt, bepaald. De veiligheid staat of valt met het beveiligingsbewustzijn speelt een rol op verschillende momenten rond een dienstverband:

- Vóór indiensttreding
  De gemeente moet waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. Dat gebeurt door een screening van de kandidaten en door hun taken en verantwoordelijkheden op dit gebied vast te leggen in het arbeidscontract.

- Bij start werkzaamheden
  Medewerkers die starten bij de gemeente volgen verplicht een programma. Een belangrijk onderdeel hierin is een e-learning in het kader van informatiebeveiliging en privacy. Zij moeten deze training binnen drie maanden hebben gevolgd en hebben afgesloten met een toets.
- Tijdens dienstverband
  De gemeente moet ervoor zorgen dat dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden en deze nakomen. De directie is hier leidend in; zij zorgen dat de kennis van de regels en verantwoordelijkheden op orde zijn bij iedereen. Daarbij hoort een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie. Ook behoort er een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
- Na uitdiensttreding
  De gemeente moet ervoor zorgen dat er duidelijkheid is over verantwoordelijkheden en taken rond informatiebeveiliging, die van kracht blijven na beëindiging of wijziging van het dienstverband. Deze zijn gedefinieerd, gecommuniceerd aan de medewerker of contractant en ten uitvoer gebracht. Zo beschermt de gemeente haar belangen.

Wetten en richtlijnen

Het integrale beleid moet passen bij de visie en het karakter van de gemeente, maar is ook onderhevig aan wet- en regelgeving.
Voor informatiebeveiliging gaat de gemeente uit van het normenkader Baseline Informatiebeveiliging Overheid en voor privacybescherming gaat de gemeente uit van de Algemene Verordening Gegevensbescherming (AVG) de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), de Wet open overheid (Woo) en de Wet politiegegevens (WPG) , die wettelijk zijn vastgesteld. Er is een verschil tussen een normenkader en een wet. Een normenkader is richtinggevend voor de maatregelen die we moeten treffen om informatiebeveiliging te waarborgen.

Informatiebeveiliging

Het doel van informatiebeveiliging is het waarborgen van de *Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)* van de informatie(systemen) van onze gemeente.
Het normenkader waar de gemeente op het gebied van informatiebeveiliging aan moet voldoen is de Baseline Informatiebeveiliging Overheid (BIO). De BIO helpt proceseigenaren in de organisatie bij het nemen van hun verantwoordelijkheid in informatiebeveiliging.
Vanuit de BIO is een aantal eisen opgelegd waar de gemeente zorg voor moet dragen, naast het opstellen van dit informatiebeveiligingsbeleid en de organisatie ervan. Hoe dit operationeel vorm krijgt, is vastgelegd in hoofdstuk 3. De norm vanuit de BIO is dat iedere gemeente maatregelen moet nemen om hieraan te voldoen. Maatregelen hebben betrekking op:

- Veiligheid medewerkers
  De gemeente moet waarborgen dat medewerkers en contractanten geschikt zijn voor hun rol. Zij moeten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen. Wordt een contract gewijzigd of beëindigd, dan beschermt de gemeente haar belangen.
- Beheer van bedrijfsmiddelen

We moeten de bedrijfsmiddelen van de gemeente identificeren en definiëren passende verantwoordelijkheden om het risico op misbruik van bedrijfsmiddelen te verkleinen.

- Toegangsbeveiliging
  De gemeente moet zorgen dat toegang tot informatie en systemen voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.
- Cryptografie
  We moeten zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen en er geen misbruik plaatsvindt.
- Fysieke beveiliging en beveiliging van de omgeving
  De gemeente moet zorgen dat de fysieke veiligheid ván en ín alle gemeentelijke locaties is gewaarborgd. Er moet beveiliging zijn om binnen te komen en beveiliging in de panden zelf. Denk aan het gebruik van pasjes, vergrendelen van systemen en het ophalen van bezoekers.
- Beveiliging bedrijfsvoering
  De gemeente moet maatregelen nemen om Informatie en informatie verwerkende faciliteiten te beschermen tegen malware, en eventuele gebeurtenissen vastleggen en bewijs verzamelen.
- Communicatiebeveiliging
  De hierboven genoemde bescherming waarborgen en handhaven, zodat in- en extern uitgewisselde informatie niet wordt aangetast of gaat verloren tijdens transport.
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
  Door te waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus, verlagen we het risico dat kwetsbaarheden ontstaan op beschikbaarheid, integriteit en vertrouwelijkheid.
- Leveranciersrelaties
  De gemeente beschermt bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers en het overeengekomen niveau van informatiebeveiliging en dienstverlening. Zo wordt inbreuk op de integriteit, vertrouwelijkheid en beschikbaarheid voorkomen.
- Beheer van informatiebeveiligingsincidenten
  We hanteren een consistente, efficiënte en doeltreffende aanpak om informatie-beveiligingsincidenten te beheren, inclusief communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
  Sommige processen moeten te allen tijde kunnen doorgaan. Afdeling burgerzaken doet bijvoorbeeld de uitwijktest; in geval van nood moet de dienstverlening van burgerzaken op een andere locatie kunnen worden voortgezet. Dat geldt overigens voor alle cruciale processen, zoals het uitbetalen van financiële uitkeringen, dienstverlening in het sociaal domein en iets eenvoudigs als vuil ophalen, mocht het nodig zijn om uit te wijken naar een andere locatie dan worden geen concessies aan de veiligheid gedaan.
- Naleving
  De gemeente voorkomt schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen rond informatiebeveiliging en beveiligingseisen. Informatiebeveiliging wordt geïmplementeerd en uitgevoerd volgens de beleidsregels en procedures van de organisatie.
- Op peil houden
  De gemeente evalueert eens per vier jaar het informatiebeveiligingsbeleid. Zo wordt continuïteit gewaarborgd en blijft de beveiliging op peil.

Privacybescherming

Voor de bescherming van privacy gebruikt de gemeente de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG (UAVG) en de Wet politiegegevens (WPG). Het beveiligen van informatie en het borgen van privacy is een continu proces, waarbij we steeds de Plan-Do-Check-Act cyclus doorlopen.
Het privacy beleid geeft in hoofdlijnen weer wat de gemeente doet met informatie van en over haar medewerkers. Er is een aantal voorwaarden van belang voor adequate privacybescherming:

- Transparantie: welke persoonsgegevens van de betrokkenen worden verwerkt en of er doorgifte is.
- Doelbeperking: de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld en mogen niet voor andere zaken gebruikt worden.
- Gegevensbeperking: enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld.
- Juistheid: de persoonsgegevens moeten correct zijn en blijven.
- Bewaarbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- Integriteit en vertrouwelijkheid: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- Verantwoording: de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen. Het college is uiteindelijke verantwoordelijk voor de privacybescherming.

AUTORITEIT
PERSOONSGEGEVENS

Nieuwe privacywetgeving vanaf 25 mei 2018
De AVG in een notendop

Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag

- Toestemming van de gebruiker
- Vitale belangen
- Wettelijke verplichting
- Overeenkomst
- Algemeen belang
- Gerechtvaardigd belang

Het begint aan de tekentafel
Zorgvuldigheid

- Functionaris gegevens-bescherming
- Privacy by design
- Impact assessment

Technische en organisatorische maatregelen
Verplichtingen

- Register met alle verwerkingen
- Gegevens-beschermingsbeleid
- (Digitale) beveiliging

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen

- Recht om in te zien
- Recht om te wijzigen
- Recht om vergeten te worden
- Recht om gegevens over te dragen
- Recht op informatie

De AVG geldt vanaf 25 mei 2018

Gegevens zijn beschermd!

U heeft een goed privacyverhaal

- Voor uw doelgroep
- Voor de Autoriteit Persoonsgegevens

De beveiligingsorganisatie

De aanwezigheid van een beveiligingsorganisatie is essentieel bij het initiëren, implementeren en borgen van beveiliging binnen de gemeente. Dat hangt niet alleen af van systemen, maar ook van medewerkers. Naast richtlijnen die alle medewerkers volgen, worden ook specifieke rollen, taken en verantwoordelijkheden toegekend.

College eindverantwoordelijk

De gemeente Oosterhout gebruikt een 'Top-Down approach'; de hoogste verantwoordelijkheid ligt bij het College van B&W. Het college heeft een kaderstellende rol en moet richting geven aan de beveiligingsdoelstellingen. De portefeuillehouder informeert de Gemeenteraad over deze doelstellingen en andere beveiligingsonderwerpen. Daarnaast is het college verantwoordelijk voor het aanstellen van een Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG).
De CISO en de FG ondersteunen bestuur en organisatie vanuit een onafhankelijke positie. Zij adviseren (on)gevraagd, stellen organisatiebreed beleid op en coördineren de implementatie. Ook ondersteunen zij bij het uitvoeren van risicoanalyses. Ten slotte verzorgen zij ook integrale statusrapportages, monitoren zij de naleving en doen zij voorstellen voor verbeteringen. Al met al fungeren de CISO en FG als overkoepelend aanspreekpunt en zijn zij ervoor verantwoordelijk dat de beveiligingsorganisatie goed functioneert.

RACI-matrix

Het geheel aan verantwoordelijkheden en taken ten aanzien van beveiliging is vastgelegd in een RACI-matrix (zie onderstaande tabel 1). De RACI-matrix geeft een overzicht van de betrokken rollen, functies en bijbehorende verantwoordelijkheden bij beveiliging. Deze verantwoordelijkheden zijn in lijn met de mandaatregeling.
De beveiligingsorganisatie bestaat uit zowel rollen als functies (gemarkeerd met een ster*).
RACI staat voor:

- R (Responsible) = verantwoordelijk voor de uitvoering = Uitvoerend
- A (Accountable) = eindverantwoordelijk, heeft eindoordeel = Beslisser
- C (Consulted) = iemand die vooraf geraadpleegd wordt = Adviseur
- I (Informed) = iemand die achteraf geïnformeerd wordt = Geïnformeerde

In- en externe factoren

Ook in de aanpak van informatiebeveiliging en privacybescherming kan de gemeente beïnvloed worden door in- en externe factoren. Een paar voorbeelden:

- Er kan nieuwe wet- en regelgeving komen, zoals de Omgevingswet. Of denk aan de Wet Open Overheid. Ook de AVG en de UAVG zijn een wettelijk kader.
- Technologische ontwikkelingen kunnen ervoor zorgen dat de gemeente anders omgaat met informatiebeveiliging. Denk bijvoorbeeld aan het verplaatsen van informatie naar de cloud.
- Daarnaast zijn er risico's die voortvloeien uit cyberaanvallen. Hackers worden slimmer en professioneler en cyberaanvallen verlopen geavanceerder.

3. OPERATIE

Als strategie, beleid en tactiek zijn bepaald, draagt de gemeente zorg voor de uitvoering in de praktijk. Zo wordt het beveiligingsbeleid geoperationaliseerd. Een proces dat nooit stopt; het beveiligen van informatie en het borgen van privacy is een continu proces dat onderhevig is aan allerlei factoren.
In de operatie moet de gemeente dus flexibel, alert en doeltreffend te werk gaan om de continuïteit en het niveau van informatiebeveiliging te waarborgen.

Afzonderlijke jaarplannen

Door ieder jaar een nieuw operationeel plan te schrijven, is het mogelijk om snel in te kunnen spelen op de actualiteit en andere ontwikkelingen. Het maakt de gemeente flexibeler en daardoor veiliger. Hoewel het beveiligingsbeleid integraal is, maken de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) afzonderlijke jaarplannen. Uiteraard zijn die wel in overleg samengesteld en op elkaar afgestemd.
De inhoud van het jaarplan verschilt van jaar tot jaar, maar is altijd gebaseerd op een aantal vaste ingrediënten. Diverse processen leiden ieder jaar tot een actuele versie van het jaarplan. Denk daarbij aan diverse onderzoeken en externe adviezen, zoals:

- De risicoanalyse, zoals uiteengezet in de BIO en het CIP normenkader voor privacy;
- Ontwikkelingen in de AVG;
- Adviezen van de Informatie Beveiligings Dienst (IBD);
- Onderzoeken;
- Het nationale dreigingsbeeld;
- Het focusdocument van de AP;
- Relevante info uit de risicoanalyses.

Zo worden de plannen samengesteld uit verschillende perspectieven en wordt het risicobeeld compleet. De gemeente kan zich daardoor beter beveiligen en voorbereiden op ingecalculeerde risico's. In de jaarplannen staan daarvoor actiepunten, die zijn belegd bij verschillende teams door de hele organisatie. Of het nu gaat om Facility, Advies of andere teams, de hele organisatie heeft ermee te maken.

Uitgangspunten

- Het integrale beveiligingsbeleid gaat zowel over informatiebeveiliging als over privacybescherming, maar beide krijgen wel een apart jaarplan. De CISO en FG kiezen daarbij samen de speerpunten en bespreken het met elkaar. Ook de teamleiders wordt gevraagd welke punten moeten worden meegenomen.
- De hoogste risico's worden het eerst aangepakt, in beide jaarplannen. De prioritering vloeit voort uit de GAP-analyse op privacy en informatiebeveiliging en wordt afgestemd met alle teamleiders.
- In de jaarplannen wordt duidelijk gemaakt hoe de gemeente groeit op de volwassenheidsladder.
- De jaarplannen moeten aansluiten op de ambities van de gemeente, aangepaste of aanvullende wetgeving en het focusdocument dat iedere drie jaar wordt opgesteld door de Autoriteit Persoonsgegevens.

- Complexe vraagstukken worden generiek behandeld. De CISO en FG adviseren hierbij en controleren hoe de organisatie zich houdt.
- Beide afdelingen maken gebruik van tools. Informatiebeveiliging werkt met een ISMS (Information Security Management System) en Privacy werkt met een PMS (Privacy Management System). Hiermee wordt gestructureerd vorm gegeven aan de PDCA-cyclus. Het is een professionele tool, die ook tijdig signalen geeft dat er een onderdeel getoetst moet worden.

Bijlage 1 RACI matrix

Verantwoordelijkheden & taken en rollen beveiligingsorganisatie	College B&W	Directie	Teamleiders	FG	PO*	CISO*	Informatiebeveiligings controller
Integraal eindverantwoordelijk voor de beveiliging van informatie en bescherming van privacy in de gemeente	A						
Opstellen van kaders o.b.v. organisatiedoelstellingen en wet & regelgeving	A	R		C	R	C	I
Beheer van het register van verwerkingen	A	I	C	C	R		
Op basis van betrouwbaarheidseisen classificatie voor de eigen informatiesystemen vaststellen;		I	A	C	R	C	I
Het uitvoeren van DPIA's en risicoanalyses		I	A	C	R	C	I
De keuze en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen en DPIA's en risicoanalyses		I	A	C	R	C	I
De implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen DPIA's en risicoanalyses			A	C	R/C	C	
Controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden				A/R	R/C	A/R	
Evalueren periodiek beleidskaders en stellen deze waar nodig bij.				A/R	R/C	A/R	
Sturen op privacy en beveiligingsbewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn);	A	R	R	R	R	R	R
Rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.				A/R	R	A/R	
Het verzorgen van advies bij vragen uit de organisatie/ nieuwe projecten				A/R	R	A/R	

Tabel: RACI-matrix verantwoordelijkheden, taken en rollen beveiligingsorganisatie

- **R** (Responsible) = verantwoordelijk voor de uitvoering = Uitvoerend
- **A** (Accountable) = eindverantwoordelijk, heeft eindoordeel = Beslisser
- **C** (Consulted) = iemand die vooraf geraadpleegd wordt = Adviseur
- **I** (Informed) = iemand die achteraf geïnformeerd wordt = Geïnformeerd

*Deze rollen zijn bij de Equalit share en bij gemeente Oosterhout belegd

Informatiebeveiligingscontroller

De informatiebeveiligingscontroller heeft de volgende taken:

- Onderhouden van contacten met overheidsinstanties en belangengroepen aangaande informatiebeveiliging.
- Organisatiebrede toetsing en auditing van de naleving van het informatiebeveiligingsbeleid;
- Toetsen/bewaken van het niveau van informatiebeveiliging;
- Toetsen op het feit dat informatiebeveiliging een onderdeel uitmaakt van het informatiemanagement;
- Evalueren van beveiligingsincidenten;
- Benoemen van en adviseren over verbetermaatregelen vanuit de verschillende toetsen;

CISO gemeente Oosterhout

De informatiebeveiligingscoördinator/ CISO heeft de volgende taken:

- Opstellen algemeen beleid informatiebeveiliging;
- Overkoepelende en organisatiebrede risicoanalyses uitvoeren;
- Jaarlijks opstellen overkoepelend informatiebeveiligingsplan;
- Classificatie van de informatiehuishouding opstellen en de informatie toewijzen aan een classificatie;
- Coördinatie informatiebeveiligingsvraagstukken;
- Coördinatie informatiebeveiligingsincidenten;
- Coördinatie informatiebeveiliging derde partijen (leveranciers);
- Organisatiebreed uitdragen informatiebeveiliging in de organisaties door o.a. communicatie, trainingen en bewustzijnscampagnes;
- Het bijdragen aan jaarlijkse afdelingsplannen op het gebied van informatiebeveiliging;
- Het gevraagd en ongevraagd adviseren over strategie, beleid en uitvoeringsrichtingen op het gebied van informatiebeveiliging o.a. naar aanleiding van besluitvorming met gevolgen voor continuïteit en informatiebeveiliging;
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging en het onderhouden van contacten met overheidsinstanties en belangengroepen aangaande informatiebeveiliging;
- Coördinatie van het ENSIA-verantwoordingsproces;

- Zorgt voor rapportage aan management, directie, College B&W en Raad over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en controles.

Functionaris gegevensbescherming

De FG houdt toezicht op de gegevensverwerking in de organisatie, in het bijzonder van de persoonsgegevens. De FG heeft de volgende taken:

- AVG uitleggen aan de organisatie
- WPG uitleggen aan de organisatie;
- Privacybeleid onderhouden;
- Privacy werkzaamheden coördineren;
- Verantwoordelijkheid dragen voor het register van gegevensverwerkingen;
- Toezien op het naleven van bijbehorende verplichtingen zoals verwerkersovereenkomsten;
- Coördineren bij een verzoek van inzage (of andere rechten van betrokkenen);
- Toezien op de toegankelijkheid van burgers tot hun gegevens;
- Verantwoordelijkheid dragen voor de afhandeling en evaluatie van datalekken en het inrichten van een procedure;
- Ontwerpen toetsen en voorstellen doen vanuit het oogpunt van privacybescherming;
- Risico's signaleren op het gebied van bescherming van persoonsgegevens;
- Coördineren van Privacy Impact Assessments (PIA's);
- Behandelen van vragen en klachten van mensen binnen en buiten de organisatie;
- Aanspreekpunt zijn voor de Autoriteit persoonsgegevens (AP);
- Jaarlijks opstellen van een rapport op voor het college en directie over de uitvoering van de privacyregelgeving door de organisatie;
- Zorgen voor bewustwording en het in stand houden van de bewustwording.

Op een aantal sleutelplekken in de organisatie zijn beveiligingsrollen benoemd die decentraal bij de afdelingen werken. Dit betreft de functie van Security Officer Suwinet, Beveiligingsfunctionaris Reisdocumenten en Rijbewijzen, CISO Equalit en de Privacy Officers van Equalit en het stadhuis.

Security Officer Suwinet

De Security Officer Suwinet beheert en beheerst beveiligingsprocedures en- maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De taken van de Security Officer Suwinet zijn:

- Bevorderen en adviseren over de beveiliging van Suwinet;
- Verzorgen van rapportages over de status van de Suwinet maatregelen;
- Controleren dat de beveiliging van de Suwinet maatregelen worden nageleefd;
- Evalueren van de uitkomsten van controles;
- Doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.

De Security Officer Suwinet rapporteert rechtstreeks aan Directieteam en proceseigenaar.

Beveiligingsfunctionaris reisdocumenten en rijbewijzen

De beveiligingsfunctionaris reisdocumenten en rijbewijzen is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures reisdocumenten en rijbewijzen. Wegens nauwe overlap in de praktijk zal de beveiligingsfunctionaris, als onderdeel van zijn functie, ook de verantwoordelijkheid dragen voor de rol van beveiligingsfunctionaris BRP. Taken van de beveiligingsfunctionaris reisdocumenten en rijbewijzen zijn:

Organisatie van de beveiliging

- Het (laten) ontwikkelen, onderhouden en aanpassen van bestaande en nieuwe beveiligingsprocedures;
- Het (laten) bekendmaken en toelichten van nieuwe/gewijzigde procedures bij medewerkers;
- Het (laten) verzorgen van de beveiligingsonderwerpen tijdens het werkoverleg;
- Het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en -processen.

Onderzoek naar de status van de beveiliging

- De controle (steekproefsgewijs) op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende reisdocumenten en rijbewijzen mede aan de hand van de normeringen zoals beschikbaar gesteld in de Kwaliteitsmonitor;
- De controle op een juiste afhandeling van de zelfevaluatie zoals deze beschikbaar is gesteld in de Kwaliteitsmonitor;
- Het (laten) actualiseren van het beveiligingsplan reisdocumenten en rijbewijzen op basis van deze controles en het overkoepelende informatiebeveiligingsbeleid opgesteld door de CISO van Gemeente Oosterhout;
- Het bewaken van de uit te voeren acties voortkomend uit onderzoek, incidenten of uit de jaarlijkse actualisering van het beveiligingsplan;
- Het (laten) verrichten van onderzoek bij incidenten met het doel dergelijke situaties in de toekomst te voorkomen.

Rapportage en verantwoording

- Gevaarlijk gedrag medewerkers of niet volgen van procedures signaleren en bespreken en/of melden aan de burgemeester;
- Geconstateerde tekortkomingen in de beveiligingsvoorzieningen signaleren en bespreken en/of melden aan de burgemeester;
- Verbeteringen aan voorzieningen of gebruikersprocedures/afspraken voorstellen;
- Het registreren van de meldingen van beveiligingsincidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

De beveiligingsfunctionaris reisdocumenten en rijbewijzen is rechtstreeks verantwoording schuldig aan de burgemeester zonder tussenkomst van de leidinggevenden in de lijn. Het betreft een onafhankelijke rol, de beveiligingsfunctionaris is onderdeel van het platform informatiebeveiliging.

CISO Equalit

- Het vertalen van het informatiebeveiligingsbeleid Oosterhout naar passende (technische) maatregelen voor Equalit;
- Zorgdragen voor het vereiste niveau van informatiebeveiliging om te voldoen aan gestelde wet- en regelgeving;
- Controleren op de juiste uitvoering van het informatiebeveiligingsbeleid;
- Signaleren van beveiligingsrisico's op basis van risicoanalyses;
- Is bij beveiligingsincidenten onderdeel van het crisisteam;
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging;
- Verzamelen, controleren en delen audit bewijsmateriaal van Equalit ten behoeve van diverse audits bij deelnemers;
- Adviseren over te nemen beveiligingsmaatregelen, waarbij de juiste vertaling wordt gemaakt naar zowel management, de werkvloer als in projecten;
- Het rapporteren aan de leiding van Equalit over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles;
- Equalit adviseren en ondersteunen bij de implementatie van de BIO om te voldoen aan de diverse audit.

Privacy Officer stadhuis en Equalit

De informatiebeveiligingscontroller heeft de volgende taken:

- Uitvoeren DPIA bij nieuwe producten/diensten en wijzigingen;
- Privacyvraagstukken beantwoorden;
- Verwerkersovereenkomsten opstellen;

- Bewustwording creëren;
- Signaal functie bij proces verbeteringen;
- Ondersteuning bij inzage verzoeken;
- FG ondersteunen bij incidenten c.q. datalekken;
- Een rol bij het uitvoeren van de beheersmaatregelen op basis van de pcda-cyclus;
- Ondersteunen van de FG bij haar controlerende taken.

Omdat de bovengenoemde beveiligingsrollen nog niet alle sleutelposities afdekken, zullen additioneel op de onderstaande posities naast de al aangewezen privacybeheerders ook beveiligingsbeheerders aangesteld worden. De invulling van deze twee rollen is hieronder beschreven.

Informatiebeveiligingsbeheerders

De beveiligingsbeheerder is aanspreekpunt voor informatiebeveiliging binnen zijn vakgebied. De beheerder draagt bij aan de doorontwikkeling van Informatiebeveiliging en Privacy van de afdeling en de unit(s). Taken van de beveiligingsbeheerder zijn:

- Het uitdragen en adviseren over informatiebeveiliging binnen de afdeling, unit of cluster waarin hij\zij werkzaam is;
- Het samen met de CISO uitvoeren en begeleiden van de ENSIA-zelfevaluatie en verantwoording binnen het betreffende vakgebied;
- In overleg met de CISO, de organisatie te begeleiden bij en te helpen met het verder toepassen en implementeren van informatiebeveiligingsmaatregelen;
- Risicoanalyses uitvoeren voor het eigen taakveld waar nodig;
- Signalering van nieuwe ontwikkelingen, incidenten en knelpunten melden aan de CISO;
- Toetsing van afdelings-, cluster- of unitplannen op het gebied van informatiebeveiliging.

Beveiligingsbeheerders worden aangesteld op de volgende posities:

- Facilitaire zaken
- Inkoop
- Functioneel Beheer
- P&O

- GEO (BAG, BGT. BRO)
- Sportbedrijf
- Gemeentewerf

Privacybeheerders

Per vakafdeling wordt een privacybeheerder aangewezen. De privacybeheerders worden opgeleid, zodat ze de AVG kennen en de doorvertaling van deze wet kunnen maken voor de eigen vakafdeling. Taken van de privacybeheerders zijn:

- Informeren en adviseren van eigen afdeling over de wijze waarop optimaal gebruik van informatie kan worden gemaakt. Hierbij zorgdragend voor de Privacy en bescherming van persoonsgegevens binnen de vakafdeling;
- Bijdragen aan de doorontwikkeling van Informatiebeveiliging en privacy van de afdeling en de unit(s) onder andere door, in overleg met de FG (functionaris gegevensbescherming), de organisatie te begeleiden bij en helpen met het verder toepassen en implementeren van termen als ‘privacy by design’ en ‘privacy by default’;
- Aanspreekpunt zijn, binnen de eigen afdeling, van het door de FG opgestelde privacybeleid;
- Bijdragen aan het opstellen en controleren van de verwerkersovereenkomsten van de afdeling. De finale controle gebeurt altijd samen met de FG;
- Ondersteunen van de proceseigenaar bij het in kaart brengen van de risico’s, bijvoorbeeld bij de uitvoering vaneen Privacy Impact Assessment (PIA).
- Op de werkvloer adviseren van vakafdelingen en vragen beantwoorden zoals:
    - Hoe kunnen we deze gegevens delen?
    - Aan welke regels dienen we ons te houden?
    - Welke maatregelen moeten we toepassen/de externe partij opleggen?
    - Welke de wettelijke grondslag hoort bij deze processen (en doelbinding)?
    - Is er een verwerkersovereenkomst nodig in deze samenwerking/uitbesteding?