gemeente Oosterhout

Beleid voor informatieveiligheid en privacybescherming, gemeente Oosterhout 2019-2021

Beleid voor informatieveiligheid en privacybescherming, gemeente Oosterhout
2019-2021

Versie: Definitief
Datum: 13 juni 2019
Auteur: Mandy de Haas en Jolanda Kerremans

Inhoud

1 Een veilige en betrouwbare gemeente!

Informatie en gegevens zijn, net als bijvoorbeeld wegen en bruggen, kostbaar. Het vraagt een hoop geld om ze te produceren en te onderhouden. Het zijn belangrijke ‘assets’ voor de gemeente. Net als de buitenruimte moet ook de ‘informatieruimte’ op orde zijn. Is dit niet het geval dan verliest de gemeente aan betrouwbaarheid of kunnen zelfs gevaarlijke situaties ontstaan.

Het beheren en verwerken van informatie is de laatste decennia sterk veranderd. Daar waar de informatie vroeger op papier vastlag en kon worden opgeborgen achter slot en grendel, is de informatie tegenwoordig grotendeels (ook) digitaal beschikbaar en daarom moeilijk ‘vast te pakken’ en gemakkelijk vermenigvuldigbaar. Als je er toegang toe hebt is het erg eenvoudig en snel te verspreiden. Informatie gaat in een fractie van een seconde de aarde rond en kan in één keer beschikbaar zijn voor een grote groep mensen.

Kwaliteit en veiligheid van gegevens is dus belangrijk. Bij persoonsgegevens is betrouwbaarheid van de gemeente wellicht nóg belangrijker. Inwoners, ondernemers en medewerkers moeten ervan kunnen uitgaan dat de door de gemeente over hen opgeslagen, aangepaste, beheerde en gedeelde gegevens in betrouwbare handen zijn. Zaken zoals identiteitsfraude, onjuist verzonden brieven en stigmatisering van mensen of groepen willen we te allen tijde voorkomen. Betrouwbaarheid is ook essentieel bij het delen van gegevens met ketenpartners.

Landelijk is er de laatste jaren veel aandacht voor privacybescherming en informatiebeveiliging. Voor gemeenten is de Baseline Informatiebeveiliging Gemeenten (BIG) ontwikkeld en verplicht gesteld en op het gebied van privacy is de Algemene Verordening Persoonsgegevens (AVG) ingevoerd.

Met andere woorden beveiliging van informatie en bescherming van privacy zijn belangrijk voor de betrouwbare gemeente die we willen zijn. Omdat betrouwbaarheid niet vanzelf komt, nemen we veiligheidsaspecten mee bij ontwerpen en aanpassingen op het gebied van mens, proces, fysieke- en virtuele omgeving. We zorgen ervoor dat we niet onbewust risico’s lopen. We kennen de risico’s en wegen deze af zodat we op een verantwoorde manier, uitlegbaar, bewust risico kunnen nemen. Met andere woorden: bewust risico nemen betekent dat we goed kijken naar wat er op de gemeente afkomt zodat we ons bewust zijn van de mogelijke risico’s. Of een risico klein of groot is hangt af van zowel de kans dat het optreedt als de gevolgen ervan wanneer het optreedt. Als we vinden dat een risico aanvaardbaar is dan accepteren we dat bewust. We wegen de kosten af die ontstaan bij optreden van het risico en de kosten, reputatieschade of juridische gevolgen die gepaard kunnen gaan met het nemen van maatregelen om een bepaald risico tegen te gaan.

In dit beleid worden privacybescherming en informatiebeveiliging integraal opgepakt. Daarom spreken we in het vervolg van dit beleidsplan over het begrip beveiliging en niet over privacybescherming en informatiebeveiliging afzonderlijk.

1.1 Wat is beveiliging?

Er zijn veel raakvlakken tussen informatiebeveiliging en privacybescherming. Daarom benaderen beveiliging zoveel mogelijk integraal. Dat scheelt overlap en dus tijd en kosten. Ondanks de integrale benadering hebben de deelterreinen van beveiliging: informatiebeveiliging en privacybescherming, wel ieder hun eigen invalshoek. De onderwerpen completeren elkaar, maar vallen niet één op één samen. Gegevens, waaronder persoonsgegevens, kunnen alleen beschermd worden wanneer informatiebeveiliging op orde is. Informatiebeveiliging legt de focus wat dat betreft op een bredere set van gegevens en middelen en gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle in de gemeente aanwezige gegevens. Bij privacybescherming ligt de focus anders en gaat het behalve over het beveiligen van persoonsgegevens tegen inbreuken, ook over de vraag of persoonsgegevens wel moeten worden verzameld. Privacybescherming gaat uit van het beperken van het verzamelen en gebruiken van persoonsgegevens tot het minimaal noodzakelijke. Een ander verschil is dat privacybescherming de rechten van betrokkenen waarborgt, zoals bijvoorbeeld inzagerechten. De kaders voor beveiliging komen voort uit wet- en regelgeving op het gebied van informatiebeveiliging en privacybescherming. In deze paragraaf geven we de kaders voor informatiebeveiliging en privacybescherming zoals die vanuit deze wet- en regelgeving zijn gegeven.

1.1.1 Informatiebeveiliging

De landelijke kaders voor informatiebeveiliging bij gemeenten zijn vastgelegd in de Baseline Informatiebeveiliging Gemeenten (BIG) en de opvolger ervan, de Baseline Informatiebeveiliging Overheid (BIO). Beide baselines zijn geënt op de normen ISO 27001 en ISO 27002. De uit de BIG volgende doelen voor Informatiebeveiliging zijn: het waarborgen van de **Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)** van de informatie(systemen) van onze gemeente.

We lichten de begrippen hieronder kort toe:

- **Beschikbaarheid:** Het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers. Beschikbaarheid is van belang voor de continuïteit in dienstverlening en bedrijfsvoering;
- **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.

1.1.2 Privacybescherming

Het wettelijk kader voor privacybescherming wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG). Implementatie van de AVG zorgt ervoor dat privacybescherming van inwoners en medewerkers geborgd is.

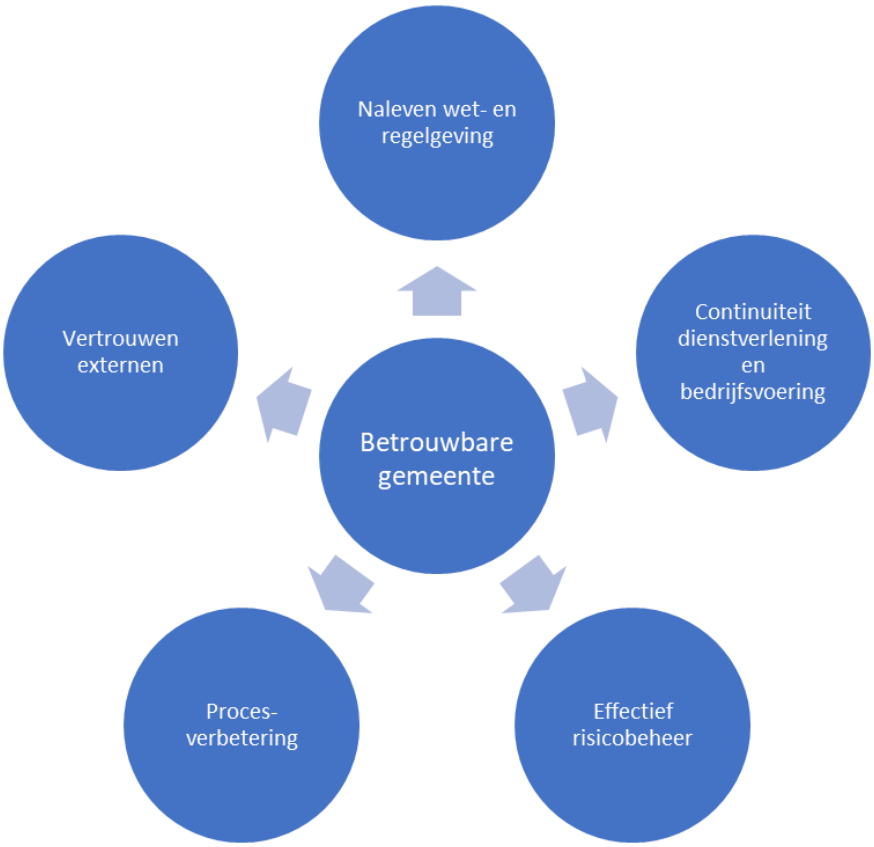
De AVG geeft zes principes voor privacybescherming, namelijk:

- **Rechtmatigheid, behoorlijkheid, transparantie:** Persoonsgegevens worden verwerkt op een manier die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- **Doelbinding:** Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en vervolgens alleen verder verwerkt worden wanneer er sprake is van een verenigbaar doel;
- **Dataminimalisatie:** Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is voor het doel. Proportionaliteit en subsidiariteit worden gebruikt om deze afweging te maken.
- **Juistheid:** Er moet voortdurend worden nagegaan of de persoonsgegevens die de gemeente van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn, dan moeten ze worden gewijzigd of verwijderd;
- **Opslagbeperking:** Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking.
- **Passende en technische of organisatorische maatregelen:** De gemeente dient er voor te zorgen dat er een goede beveiliging van (persoons) gegevens is, door het nemen van passende technische of organisatorische maatregelen. We moeten er voor zorgen dat ongeoorloofde toegang tot- en gebruik van persoonsgegevens voorkomen wordt. Kortom we borgen de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens.

1.2 Onze visie op beveiliging

Oosterhout is een betrouwbare gemeente waar gegevens en informatie van inwoners, ondernemers, personeel, partners en andere betrokkenen veilig, vertrouwelijk en daarmee zorgvuldig worden behandeld. Privacy wordt te allen tijde beschermd. De gemeente heeft zicht op de door haar, of door derden voor haar, verwerkte gegevens en respecteert de rechten van betrokkenen.
Door het borgen van beveiliging toont de gemeente haar betrouwbaarheid. Deze betrouwbaarheid komt tot uiting op de volgende onderwerpen:

- **De gemeente leeft wet- en regelgeving na**. De gemeente Oosterhout verwerkt veel (persoons)gegevens. Veel van deze gegevens zijn bijzonder gevoelig en complex van aard. Door integraal beveiligingsbeleid te formuleren voldoet de gemeente aan eisen die zijn gesteld vanuit wet- en regelgeving. Meer specifiek voldoet de gemeente hiermee aan de AVG en BIG/BIO. Hiermee wordt onder meer voldaan aan de verantwoordings- en transparantieplicht (ENSIA en AVG). Daarnaast worden passende organisatorische en technische beveiligingsmaatregelen getroffen in de processen;
- **De gemeente levert continuïteit in dienstverlening en bedrijfsvoering.** Het beveiligingsbeleid draagt bij aan het voorkomen van verstoringen en daarmee aan een ononderbroken dienstverlening en bedrijfsvoering. Verstoringen in continuïteit kunnen optreden wanneer bij bijvoorbeeld stroomuitval, brand of wanneer aan internet verbonden systemen worden gehackt zoals gemalen en stoplichten;
- **De gemeente zorgt voor effectief risicobeheer.** Door zorgvuldige afweging te maken tussen mogelijke risico's, het effect ervan en de kosten om deze risico's te voorkomen gaat de gemeente op een effectieve manier om met haar middelen en kan zij bewust risico's nemen;
- **De gemeente verbetert haar processen.** Het beveiligingsbeleid draagt bij aan het inzicht in huidige verwerkingen, het applicatielandschap en informatie uitwisselingen. Met deze kennis kunnen processen worden gestroomlijnd en verbeterd;
- **De gemeente genereert vertrouwen in haar informatieverwerking- en deling**. Behalve algemene betrouwbaarheid draagt het beveiligingsbeleid ook bij aan vertrouwen in de manier waarop zij omgaat met de (persoons)gegevens die zij verwerkt en/of deelt met ketenpartners. Ook de wijze waarop de gemeente de privacyrechten van burgers waarborgt draagt bij aan de *betrouwbaarheid van de gemeente.*



Figuur 1: Visie op beveiliging

1.3 Uitgangspunten beveiliging

De gemeente Oosterhout geeft richting aan haar visie middels onderstaande uitgangspunten. Deze uitgangspunten zijn geformuleerd op basis van bovenstaande visie en de globale omgevingsanalyse die is beschreven in hoofdstuk 2.

De uitgangspunten voor beveiliging zijn:

1. Integrale blik op beveiliging;
2. Beveiliging begint bij organisatiebewustzijn;
3. Waarborgen (privacy)rechten van betrokkenen;
4. Er is een actueel overzicht van gegevensverwerkingen;
5. Bedrijfsmiddelen zijn geïdentificeerd en geclassificeerd;
6. Bedrijfsmiddelen hebben een eigenaar;
7. Er zijn passende technische- en organisatorische maatregelen genomen;
8. We zien toe op het naleven van maatregelen;
9. Bewust risico nemen in plaats van onbewust risico lopen;
10. Beveiliging wordt standaard meegenomen bij het ontwerpen en aanpassen van processen;
11. Beveiliging is geïntegreerd in processen;
12. Beveiligingsincidenten en datalekken worden vastgelegd en gemeld;
13. Beveiliging bij derden is geborgd;
14. Transparantie in de persoonsgegevens die wij verwerken;
15. Fysieke beveiliging is op orde;
16. Continuïteit in dienstverlening en bedrijfsvoering is gewaarborgd;
17. We ontwikkelen langs de volwassenheidsladder voor beveiliging.

We lichten de uitgangspunten hieronder verder toe.

1. **Integrale blik op beveiliging**
   Vanwege de nauwe samenhang tussen informatieveiligheid en privacybescherming benaderen we deze integraal. Er is één gezamenlijk beleid. Jaarlijkse risicoanalyse, planvorming en verantwoording worden gestroomlijnd en zoveel mogelijk gelijk getrokken.

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. Het belang van bewustzijn geldt zowel voor de mensen die erover gaan (sturing), de mensen die met gegevens werken (uitvoering) als voor de mensen die gegevens beheren en zorgen voor technische maatregelen (beheer).

3. **Waarborgen van (privacy)rechten van betrokkenen**
   Organisaties moeten zorgen dat mensen hun rechten kunnen uitoefenen. Het gaat dan om bestaande rechten, zoals het recht op inzage en verwijdering van hun gegevens en het recht om bij de overheid bekende en beschikbare gegevens niet opnieuw te hoeven verstrekken. Daarnaast gaat het ook om nieuwe rechten, zoals het recht op dataportabiliteit; het recht om persoonsgegevens te ontvangen die een organisatie van hen heeft, deze zelf op te slaan of door te geven aan een andere organisatie. Ook moeten organisaties er rekening mee houden dat betrokkenen bij de AP klachten kunnen indienen over de manier waarop organisaties met hun gegevens omgaan. Het volledige overzicht van rechten van betrokkenen is te vinden in paragraaf 2.2.3.

4. **Er is een actueel overzicht van gegevensverwerkingen**
   Gegevensverwerkingen zijn in kaart gebracht en worden voortdurend geactualiseerd. Gedocumenteerd is welke persoonsgegevens worden verwerkt en met welk doel en grondslag dit gebeurt, waar deze gegevens vandaan komen en met wie ze worden gedeeld. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht van de AVG. Het register is ook nodig wanneer betrokkenen hun privacyrechten uitoefenen. Als zij vragen hun gegevens te corrigeren of verwijderen, moet dit worden doorgeven aan de organisaties waarmee hun gegevens zijn gedeeld. Daarnaast geeft het inzicht in de te beveiligen persoonsgevoelige informatie.

5. **Bedrijfsmiddelen zijn geïdentificeerd en geclassificeerd**
   De gemeente Oosterhout beschikt over een variëteit aan middelen die noodzakelijk zijn voor goede diensteverlening en bedrijfsvoering. Deze bedrijfsmiddelen zijn niet alleen noodzakelijk, maar kunnen ook geld kosten of een bepaalde waarde vertegenwoordigen. Voorbeelden van bedrijfsmiddelen zijn:
   - informatie in de vorm van bijvoorbeeld documenten, databases, contracten, systeemdocumentatie, procedures, handleidingen, systeemlogs, plannen en programmatuur;
   - Apparatuur zoals servers, pc's, netwerkcomponenten en bekabeling;
   - Mensen en hun kennis;
   - Immateriële zaken zoals imago of reputatie van de gemeente.

   Bedrijfsmiddelen hebben een classificatie nodig om er beveiligingsniveaus op te kunnen vaststellen. Een goede registratie van bedrijfsmiddelen is noodzakelijk voor het bepalen van een passend niveau van beveiliging.
   Daarnaast is registratie soms nodig voor de verzekering, financiële verantwoording en wettelijke vereisten (zie hier bijvoorbeeld het eerdergenoemde uitgangspunt met betrekking tot de registratie van gegevensverwerkingen in het kader van de AVG).

6. **Bedrijfsmiddelen hebben een eigenaar**
   Bij de geïdentificeerde en geclassificeerde bedrijfsmiddelen zijn eigenaren benoemt. Dit is nodig omdat eigenaren bepalend zijn bij het maken van risicoafwegingen op de bedrijfsmiddelen waar zij eigenaar van zijn.

7. **Er zijn passende technische- en organisatorische maatregelen genomen**
   De maatregelen die worden genomen sluiten aan bij de kans en de gevolgen van mogelijke bedreigingen op de bedrijfsmiddelen van de gemeente. De maatregelen dragen bij aan het waarborgen van de continuïteit in dienstverlening en bedrijfsvoering. Op basis van de classificatie van bedrijfsmiddelen wordt gekeken hoe kritisch deze middelen zijn. Door toepassing van het juiste beveiligingsniveau worden onnodige kosten voorkomen. Met andere woorden: Er wordt een zorgvuldige afweging gemaakt tussen mogelijke risico's, het effect ervan en de kosten om deze risico's te voorkomen[1].

8. **We zien toe op het naleven van maatregelen**
   Naast het nemen van maatregelen zien we uiteraard ook toe op het naleven van maatregelen. Enerzijds vanuit compliance (wettelijke voorschriften) en anderzijds op het voldoende afdekken van de geïdentificeerde risico's.

9. **Bewust risico nemen in plaats van onbewust risico lopen**
   De gemeente Oosterhout hanteert als uitgangspunt voor beveiliging: 'bewust risico nemen', in plaats van 'onbewust risico lopen'. Er wordt vooruitgekeken. We voldoen uiteraard aan wet- en regelgeving. We zijn compliant. Daarnaast kijken we nu, meer dan voorheen, welke bedreigingen mogelijk op de gemeente afkomen. Daarbij bepalen we de kans 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. We nemen passende beveiligingsmaatregelen om de betreffende bedreigingen te voorkomen, of de effecten ervan te reduceren. Deze systematiek sluit aan op de overgang van de baseline informatiebeveiliging (BIG) naar de Baseline Informatiebeveiliging Overheid (BIO). In de BIO staat risicomanagement centraal en is de rol van de bestuurder en lijnmanager ten aanzien van risicomanagement explicieter dan de BIG aangaf. Het beveiligingsbeleid legt vast wie deze keuzes wanneer maakt en geeft handvatten voor het nemen van maatregelen binnen de beveiligingsprocessen. Bij processen waar met veel of bijzondere persoonsgegevens wordt gewerkt, schrijft de AVG voor dat er een DPIA uitgevoerd moet worden. Met een DPIA worden de privacyrisico´s van een gegevensverwerking in kaart gebracht. Om daar vervolgens verbetervoorstellen c.q. maatregelen aan te koppelen. Gemeente Oosterhout neemt met het uitvoeren van de DPIA´s de elementen m.b.t. informatiebeveiliging mee. Zoals eerder aangeven kan het een niet zonder het ander en dat komt hierbij duidelijk naar voren.

[1] Bij het operationaliseren van beveiligingsbeleid zijn bij het invulling geven van maatregelen, ook de *Architectuuruitgangspunten Equalit* van belang.

10. **'Pas toe of leg uit' principe**
    Gemeente Oosterhout leeft wet- en regelgeving op het gebied van beveiliging na. Echter is het naleven van wet- en regelgeving geen doel op zich. 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. Handvaten voor het maken van dergelijke risicoafwegingen, staan in een afwegingskader. De ruimte om risicoafwegingen te maken biedt de AVG ook. Dit kan door het noodzakelijkheidsvereiste (de verwerking van de persoonsgegevens moet noodzakelijk zijn om de publieke taak of wettelijke verplichting goed te kunnen vervullen) en het proportionaliteitsvereiste in acht te nemen.

11. **Beveiliging wordt standaard meegenomen bij het ontwerpen en aanpassen van processen**
    Dit principe, ook wel bekend als: beveiliging 'by design & by default', 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. Bijvoorbeeld dat we vanuit het oogpunt van privacybescherming niet meer gegevens verzamelen dan noodzakelijk is voor het doel van de verwerking en we de gegevens niet langer bewaren dan nodig. Vertegenwoordigers uit de beveiligingsorganisatie worden betrokken bij veranderingen.

12. **Beveiliging is geïntegreerd in processen**
    Beveiliging is ingebed in de organisatie en daarmee een bekend en gebruikelijk aspect in de organisatiebrede manier van werken. Rekening houden met beveiliging is een gegeven, een 'tweede natuur' van medewerkers. Het organisatiebreed benoemen van informatiebeveiligingsbeheerders naast de al aangewezen privacybeheerders draagt hieraan bij.

13. **Beveiligingsincidenten en datalekken worden vastgelegd en gemeld**
    Incidenten en datalekken worden te allen tijde vastgelegd. Bij incidenten wordt het incidentproces gevolgd. Indien een incident een datalek is dan wordt dit vastgelegd in een register bij de procedure voor datalekken. Een datalek wordt door de FG gemeld bij de Autoriteit Persoonsgegevens[2]. Zowel de gebeurtenis (incident/datalek) als de opvolging ervan worden gedocumenteerd. De wijze waarop beveiligingsincidenten en datalekken worden vastgelegd en gemeld is uitgewerkt in een werkprocedure.

14. **Beveiliging bij derden is geborgd**
    De gemeente besteedt de uitvoering van taken en het beheer van systemen op onderdelen uit aan externe partijen. Hiermee hebben ook zogenaamde 'derden' te maken met gegevens en andere bedrijfsmiddelen van de gemeente. Voorbeelden zijn de inhuur van een medewerker of het verwerken van gegevens door externe partijen. Het meenemen en borgen van beveiliging is ook hier een standaard gegeven. Borging kan op verschillende manieren gebeuren zolang wordt voldaan aan de eisen die gelden voor beveiliging. Voorbeelden van contractuele afspraken op dit gebied zijn: SLA's, verwerkersovereenkomsten, geheimhoudingsverklaringen, certificering etc. Een vast onderdeel bij aanbestedingen is het borgen van beveiliging. Bij uitbesteding van gegevensverwerking worden afspraken vastgelegd in een verwerkersovereenkomst. Er is een register van verwerkers en er zijn verwerkingsovereenkomsten afgesloten met deze verwerkers. De gemeente Oosterhout heeft een sjabloon verwerkersovereenkomst opgesteld en vastgesteld. Resultaat is dat de gemeente met de verwerkingsovereenkomsten een standaard set aan afspraken heeft waarmee veilige verwerking van de gegevens door derden is geborgd.

15. **Transparantie in de persoonsgegevens die wij verwerken**
    Basis voor gegevensvastlegging zijn de wettelijke taken van de gemeente Oosterhout. Alle gegevensverwerkingen zijn in beeld. 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

[2] Bij melden van een datalek worden de *Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679* gehanteerd. *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052*

moet voor iedereen duidelijk zijn welke personen, wanneer toegang hebben tot welke ruimten en op welke manier deze toegang wordt geregeld. Kaders voor fysieke beveiliging worden nader uitgewerkt in een specifiek beleidskader fysieke beveiliging.

17. **Continuïteit in dienstverlening en bedrijfsvoering is gewaarborgd**
De gemeente voert taken uit die direct van belang zijn voor haar inwoners. Om deze taken uit te voeren worden bedrijfsprocessen uitgevoerd die als 'kritisch' kunnen worden aangemerkt. Langdurige uitval van deze bedrijfsprocessen is vanwege de negatieve gevolgen voor de gemeente, burgers, medewerkers, bedrijven, (keten)partners en andere betrokkenen onacceptabel. Om langdurige stagnatie van de kritische bedrijfsprocessen van de gemeente te voorkomen dient een proces voor continuïteitsbeheer te worden ingericht. Onderdeel van dit proces vormt het opstellen van het continuïteitsplan. In dit plan zijn de acties vastgelegd die dienen te 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. We hanteren het model van het Centrum Informatiebeveiliging en Privacybescherming (CIP) dat de volwassenheid in vijf volwassenheidsniveaus uitdrukt. De vijf niveaus worden gedefinieerd aan de hand van de mate waarin voldaan wordt aan de beveiliging. Het CIP vertaalt de wetgeving op het gebied van privacybescherming en informatiebeveiliging naar concrete, hanteerbare normen die duidelijk aangeven waar organisaties wat moeten regelen in hun beveiligingsbeleid, de uitvoering en de controle erop. Het ambitieniveau en de te nemen stappen voor de groei worden beschreven in de jaarplannen. Zo ontstaat er een stapsgewijze aanpak, waarop de planning met bijbehorende middelen worden afgestemd.

2 Wat gaan we hiervoor doen?

2.1 Integrale benadering van beveiliging

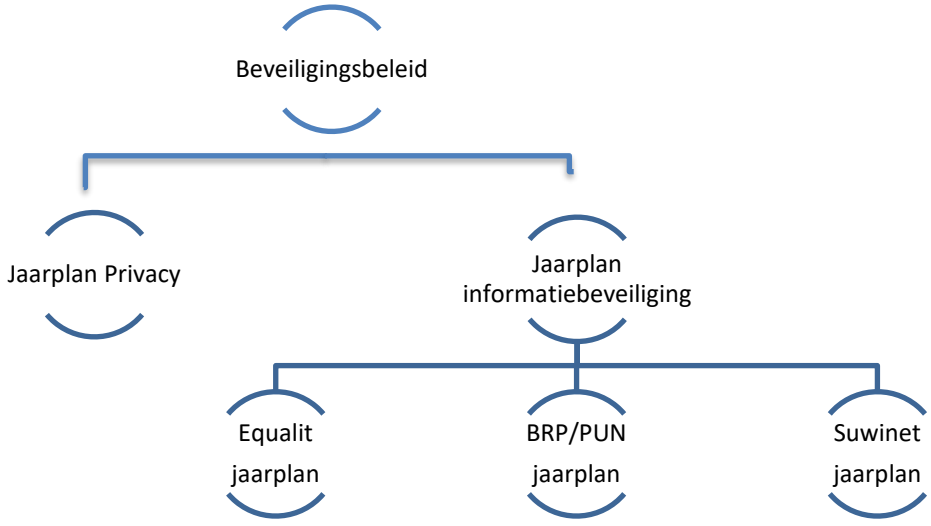
Met dit beveiligingsbeleid worden verschillende aandachtsgebieden op het gebied van beveiliging met elkaar verbonden. Daar waar voorheen beveiliging verticaal in kokers werd georganiseerd (Informatiebeveiliging, privacybescherming, Suwinet, BRP/PUN, BAG, BGT, BRO en DigiD) zijn deze gebieden met dit beleid voorzien van één strategische visie. Dat scheelt tijd en geld.

Op basis van dit beleid kunnen we efficiënt en eensluidend deelplannen formuleren. Bij verantwoording maken we gebruik van de ENSIA-systematiek. ENSIA staat voor Eenduidige Normatiek Single Information Audit. Deze landelijke systematiek wordt gebruikt voor verantwoording op meerdere domeinen en beperkt door haar eenduidigheid de administratieve lasten. De verantwoording kan daardoor efficiënter en effectiever worden uitgevoerd.

In de praktijk wordt overigens nu al hecht samengewerkt tussen de informatiecoördinator, Chief Information Security Officer (CISO) en Functionaris Gegevensbescherming (FG).

Kortom, dit beleidsplan biedt strategische kaders voor integrale beveiliging. Het beleid is gebaseerd op de per mei 2018 geldende Algemene verordening gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Gemeenten (BIG). Omdat de BIG overgaat naar de Baseline Informatiebeveiliging Overheid (BIO) anticiperen we daar nu al op in. Behalve dat het beleid aansluit bij de eisen in de AVG en de BIG/BIO biedt het beleid kaders voor de beveiliging van de domein-gerelateerde gegevens van Suwinet, BRP/PUN, BAG, BGT, BRO en DigiD. De FG en CISO beoordelen jaarlijks het beveiligingsbeleid en passen deze waar nodig aan.

Op basis van dit beleid worden de jaarlijkse risicoanalyses en beveiligings- en privacybeschermings-plannen opgesteld.



Figuur 2: Jaarplannen

Het voorgaande informatiebeveiligingsbeleid legde primair de insteek op compliance, ofwel het toetsen of voldaan werd aan de eisen vanuit wet- en regelgeving. Compliance blijft belangrijk, maar wordt voorzien van een ‘blik vooruit’. Het beleid voor informatiebeveiliging en privacybescherming legt meer dan voorheen de nadruk op het uitvoeren van risicoanalyse. Het sluit hiermee aan op landelijke

ontwikkelingen en de Baseline Informatiebeveiliging Overheid (BIO). De manier waarop de beveiliging organisatorisch wordt ingevuld is beschreven in hoofdstuk 3. We gaan daarbij ook in op de manier waarop we de kwaliteit van beveiliging borgen en de manier waarop we risicoanalyse toepassen bij beveiliging.

2.2 Globale omgevingsanalyse informatieveiligheid en privacy

2.2.1 Wet- en regelgeving

Naast het gegeven dat we een betrouwbare gemeente willen zijn, hebben we te maken met verplichtingen uit wet- en regelgeving. Het gaat hier om wetten zoals SUWI, BRP, BAG, BGT, BRO en PUN, maar ook de archiefwet en de AVG. Het beveiligingsbeleid is in lijn met het algemene beleid en de bovenstaande relevante landelijke en Europese wet- en regelgeving. Onderdeel van het takenpakket van beveiliging is het volgen van de ontwikkelingen in de wet- en regelgeving, respectievelijk het vertalen van de betreffende eisen naar één of meerdere beveiligingsmaatregelen.

2.2.2 Vooruitkijken: wat komt er op de Gemeente af?

We passen risicomanagement toe. Dit betekent dat we vooruitkijken. We identificeren en duiden ontwikkelingen en brengen eventuele dreigingen in beeld. In deze paragraaf geven we de belangrijkste ontwikkelingen aan op hoofdlijnen. Bij het bepalen van de ontwikkelingen die voor Oosterhout van belang zijn maken we gebruik van kennis die beschikbaar is bij onder andere de Informatie Beveiligingsdienst (IBD), Autoriteit Persoonsgegevens (AP) en het Centrum Informatiebeveiliging en Privacybescherming (CIP).
De IBD heeft risico's geïdentificeerd die in het algemeen gelden voor gemeenten.[3] Voorbeelden waar we in dit verband naar moeten kijken zijn:

- **Imagoprobleem beveiliging**: Laag op de politieke agenda, weinig bewustzijn en onvoldoende budget;
- **Risico's niet integraal in beeld:** De risico's die wel in beeld zijn, krijgen bovenmatig veel aandacht;
- **Basis niet op orde**: Simpele routineaanvallen zijn vaak succesvol;
- **Te weinig mensen**: Te veel werk en te weinig gekwalificeerde specialisten;
- **Complexiteit neemt toe:** Gemeenten zien kansen van innovatie, maar niet de risico's.

Voor Oosterhout zijn, bij het maken van een juiste risicoafweging, naast bovenstaande punten de komende jaren een aantal specifieke ontwikkelingen van belang, namelijk:

- **Focus op informatiegestuurd werken:** We werken informatiegestuurd. Dit betekent dat de afhankelijkheid van betrouwbare informatie verder toeneemt. Er zullen vragen opkomen om (persoons)gegevens beschikbaar te stellen of te verzamelen voor analyse. Door de beveiligingsorganisatie te betrekken bij vraagstukken op het gebied van informatiegestuurd werken kunnen we aanpassingen in dataverzameling -en bewerking integraal afwegen;
- **Beveiliging bij sub-locaties (zwembad e.a.):** Voorheen lag de focus van beveiliging in eerste plaats op de informatiehuishouding binnen het stadhuis. Echter worden ook op sub-locaties (persoons)gegevens verwerkt en is beveiliging van belang. Het is daarom belangrijk om ook de sub-locaties actief te betrekken bij beveiliging en ook voor de sublocaties, naast de al aangewezen privacybeheerders, informatiebeveiligingsbeheerders aan te wijzen. De kaders voor de fysieke beveiliging van sub-locaties worden gegeven in een nader uit te werken beleid voor de fysieke beveiliging.

De hierboven beschreven onderwerpen vragen om grote(re) betrokkenheid van de beveiligingsorganisatie en komen tot uiting in de uitwerking van het beleid, de uitgangspunten, beveiligingsorganisatie en sturing. Specifieke uitwerking vindt, na afweging van risico's, plaats in de jaarlijks op te stellen beveiligingsplannen.

2.2.3 Rechten van betrokkenen

Bij het werken met informatie heeft de gemeente te maken met een verscheidenheid aan interne rollen en externe partijen. Interne belanghebbenden zijn onder meer: medewerkers, management, bestuur, OR, inhuurkrachten en de Equalit deelnemers. De verschillende organisatieonderdelen hebben ieder

[3] *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020*, IBD VNG

hun eigen specifieke gezichtspunt. Externe belanghebbenden zijn onder meer: burgers, bedrijven, maatschappelijke partners, samenwerkingsverbanden, landelijke organen en leveranciers. Uiteraard kunnen er verschillen in belangen bestaan. Bij het maken van een risicoanalyse (per aandachtsgebied) wegen we de belangen van de interne- en externe rollen en partijen zorgvuldig mee.

Belangrijk om hier te noemen is dat in de AVG naast plichten, voor overheden en het bedrijfsleven, ook belangrijke rechten zijn meegegeven voor betrokkenen, namelijk:

- Recht op inzage: Dat is het recht van mensen om de persoonsgegevens die de gemeente over hen verwerkt in te zien;
- Recht op rectificatie en aanvulling: Het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen;
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken;
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten;
- Het recht om bezwaar te maken tegen de gegevensverwerking;
- Het recht om als organisatie persoonsgegevens over te dragen (dataportabiliteit) en;
- Het recht van mensen om ‘vergeten’ te worden (recht op vergetelheid).

Binnen de gemeente Oosterhout zijn de rechten van betrokken zo ingericht, dat betrokkenen op een makkelijke manier gebruik maken van deze rechten.

2.2.4 Op weg naar een Baseline Informatiebeveiliging Overheid (BIO)

Gemeenten hanteren de Baseline Informatiebeveiliging Gemeenten (BIG) sinds 2013 als normenkader. Het rijk, de waterschappen en de provincies hanteren hun eigen respectievelijke normen. Deze normen worden op korte termijn samen met de BIG gebundeld in de Baseline Informatiebeveiliging Overheid (BIO). De nieuwe baseline wordt daarmee het nieuwe normenkader voor alle overheden en dus ook voor de gemeente Oosterhout. De BIO is een doorontwikkeling, ofwel een ‘update’, van de nu bestaande BIG. De werkzaamheden die tot op heden voor de BIG zijn verricht zijn grotendeels in lijn met de BIO. We verwachten dat de BIO op 1 januari 2020 van kracht wordt. In het algemeen geldt dat de BIO meer risico gebaseerd is en meer aandacht aan privacybescherming besteedt dan de BIG.

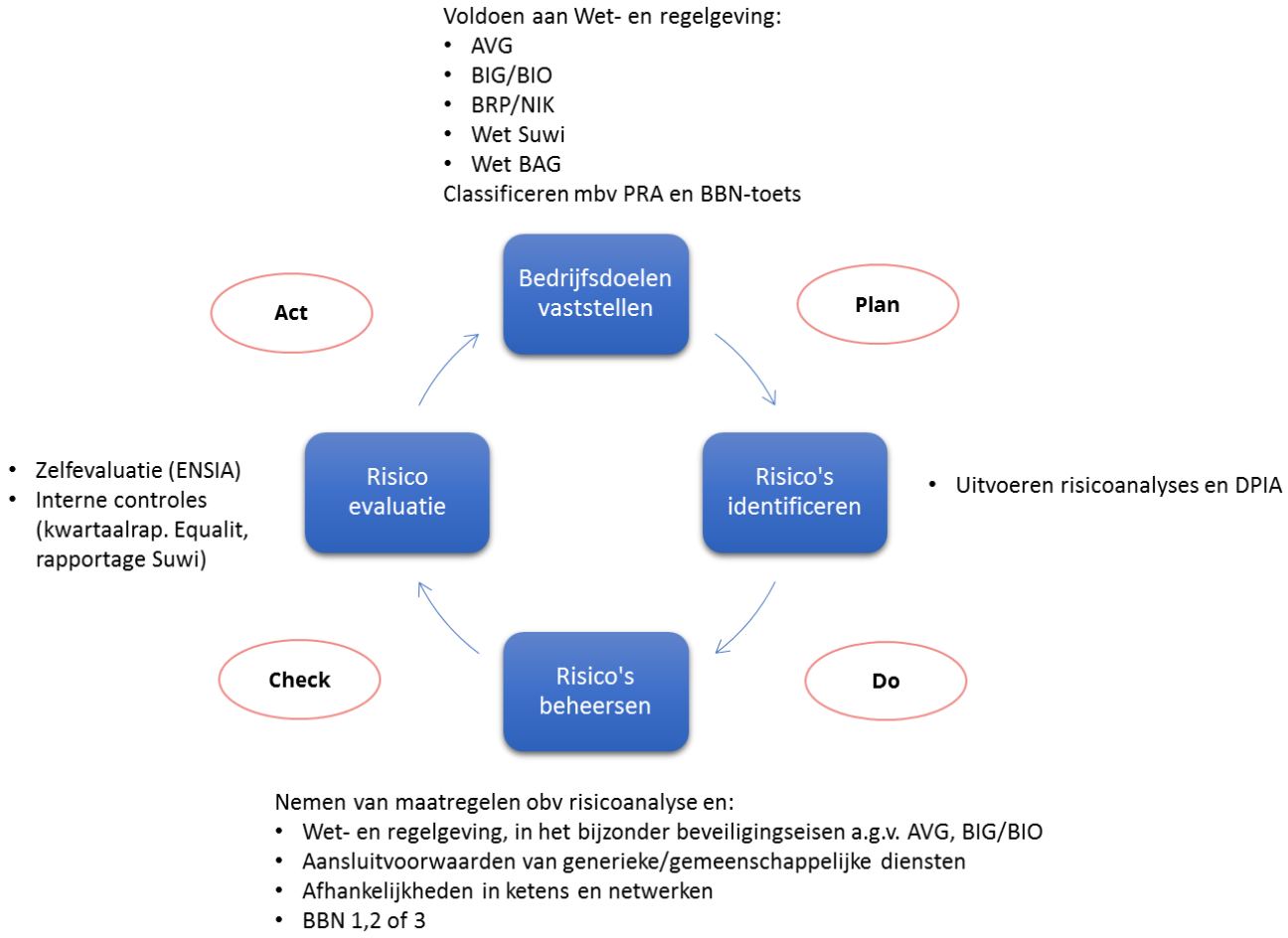
3 Hoe gaan we dit doen? Organisatie en processen beveiliging

Beveiliging is mensenwerk en raakt de hele organisatie. De mensen, hun verantwoordelijkheden en de invulling van hun rollen, vormen de basis waarop een goede beveiliging gebouwd is. We zijn bezig met het opbouwen van onze beveiligingsorganisatie. Dit doen we gestructureerd en procesmatig. In dit hoofdstuk gaan we in op het proces beveiliging en wat beveiliging betekent voor procesmatig werken. We besteden hier specifiek aandacht aan de beveiliging bij uitbesteding van processen. Vervolgens gaan we in op de rollen en verantwoordelijkheden die belangrijk zijn voor een goede beveiliging binnen de gemeente Oosterhout.

3.1 Operationaliseren van beveiligingsbeleid met behulp van een PDCA-cyclus

Het beveiligen van informatie en het borgen van privacy is geen eenmalige zaak, maar een continu proces waarbij we steeds de Plan-Do-Check-Act cyclus doorlopen. Dit doen we jaarlijks en we reviewen daarbij ook het beleid. De uitkomsten van de review van het beveiligingsbeleid bieden we via een memo aan de directie aan. Het beveiligingsbeleid wordt vastgesteld door het college van B&W en heeft een looptijd van drie jaar en wordt elk jaar opnieuw beoordeeld. De Chief Information Security Officer (CISO) en Functionaris Gegevensbescherming (FG) faciliteren en controleren dit proces. Het lijnmanagement is uiteindelijk eindverantwoordelijk en kan beveiligingsbeheerders op onderdelen verantwoordelijk maken.

De uitvoering van dit proces wordt ondersteund door een applicatie. Dit betreft een applicatie waar zowel Privacy, Governance, Risk & Compliance (GRC) en het Information Security Management System (ISMS), geïntegreerd in zijn opgenomen.



Figuur 3: Plan-Do-Check-Act cyclus beveiliging

Plan: We starten de cyclus voor verbetering van de veiligheid met het identificeren van de ontwikkelingen op het gebied van beveiliging. We bepalen daarbij wat het doel, de visie en de uitgangspunten voor beveiliging zijn.

In deze fase classificeren we ook gegevens en informatiesystemen. Met dataclassificatie bepalen we welk beveiligingsniveau van de gegevens en informatiesystemen nodig is en bekijken we welke applicaties het meest kritisch zijn voor de gemeente. Ook stellen we vast wat de risicobereidheid[4] van de organisatie is. De stakeholders kunnen aangeven welke beveiligingskwesties zij graag op de agenda willen hebben. Bestuur en management spelen bij deze integrale afweging uiteraard een belangrijke rol!

Bij het bepalen van beveiligingsniveaus leggen we de focus in eerste instantie op beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Aan de, met het management gemaakte, classificatie kennen we vervolgens basisbeveiligingsniveaus (BBN's) toe. Deze BBN's zijn nieuw voor de gemeente en komen uit de BIO. De BBN's zijn gedefinieerd op basis van de generieke schades en dreigingen en voorzien van passende beveiligingseisen.

Het bepalen van de beveiligingsniveaus zorgt ervoor dat er gepaste maatregelen genomen worden en resources op een efficiënte wijze ingezet worden, omdat de focus op het beschermen van de juiste gegevens ligt.

Do: In deze fase voeren we een risicoanalyse uit. Dit gebeurd enerzijds door het uitvoeren van een GAP-analyse op de BIG en de AVG. Welke risico's volgen uit het niet compliant zijn? Anderzijds zal er ook aandacht besteed worden aan risico's die voortkomen uit dreigingsbeelden, kwetsbaarheidsanalyses, impactanalyses en Data Protection Impact Assessment (DPIA). Bij het maken van de risicoanalyse maken we een inschatting van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook schatten we in tegen welke dreigingen de gemeente beschermd moet worden.

Het geheel aan risico's brengen we samen in een risicomatrix. Na het uitvoeren van de risicoanalyses kijken we welke risico's we kunnen mitigeren, accepteren, vermijden of overdragen. Welke beheersmaatregelen wel of niet geïmplementeerd worden bepalen we aan de hand van de gestelde doelstellingen en risicobereidheid uit de planfase.

Check: Toetsing en verantwoording voeren we uit op basis van de ENSIA. Hiermee kan de gemeente in één keer slim verantwoording afleggen over informatieveiligheid gebaseerd op de BIG/BIO (Baseline Informatiebeveiliging Nederlandse Gemeenten/Baseline Informatiebeveiliging Nederlandse Overheid). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoerings-regeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is in ENSIA samengevoegd en gestroomlijnd.

Aanvullend hierbij geldt dat specifieke controle op beveiligingsmaatregelen Suwinet ligt bij de Security Officer Suwinet en voor BRP/PUN bij de beveiligingsfunctionaris reisdocumenten en rijbewijzen.
De checkfase bevat tevens tussentijdse rapportages over voortgang van beveiliging en privacybescherming. De CISO en FG rapporteren eens per half jaar aan het college en de gemeenteraad via de P&C-cyclus in het jaarverslag en de begroting. Zij overleggen maandelijks met de directie. Beveiliging is daarnaast een vast onderdeel van het jaarlijkse auditplan. In de checkfase worden door interne control audits uitgevoerd en wordt gerapporteerd op de onderdelen: Suwinet, BRP/PUN en Equalit.

Act: De bevindingen van controles, aangevuld met een nieuwe risicoanalyse zijn weer input voor een nieuw beveiligingsplan. Ook zal het beleid opnieuw beoordeeld worden. Samen met de directie wordt gekeken of de doelstellingen en risicobereidheid nog actueel zijn.

[4] De mate van risico op breed niveau die een organisatie wil accepteren ten einde bepaalde doelstellingen te behalen.

3.2 De beveiligingsorganisatie

Volgend op de beschrijving van het hoofdproces voor beveiliging, de PDCA-cyclus, beschrijven we in deze paragraaf hoe de beveiliging van de gemeente Oosterhout is georganiseerd. In de eerste paragraaf worden verantwoordelijkheden en taken toekgekend. In de tweede paragraaf wordt de werking van de beveiligingsorganisatie verder toegelicht aan de hand van een overlegstructuur. De aanwezigheid van een beveiligingsorganisatie is essentieel bij het initiëren, implementeren en borgen van beveiliging binnen de gemeente.

3.2.1 Verantwoordelijkheden & taken en rollen beveiligingsorganisatie

De gemeente Oosterhout maakt gebruik van een 'Top-Down approach'. Dit houdt in de hoogste verantwoordelijkheid ligt bij het College van B&W. Het college heeft een kaderstellende rol en dient richting te geven aan de beveiligingsdoelstellingen. De portefeuillehouder informeert de Raad 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.

Het geheel aan verantwoordelijkheden en taken ten aanzien van beveiliging is vastgelegd in een RACI-matrix (zie onderstaande tabel 1). In de RACI-matrix wordt een overzicht gegeven van de betrokken rollen, functies en bijbehorende verantwoordelijkheden bij beveiliging. RACI is een model waarin de betrokkenheid van deelnemers binnen een proces eenvoudig en eenduidig inzichtelijk kan worden gemaakt.

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

De beveiligingsorganisatie bestaat uit zowel rollen als functies. In de RACI-matrix is een ster* bij de functies geplaatst. Indien er geen ster* geplaatst is betreft het een rol. In bijlage 2 zijn uitgebreide rol- en functiebeschrijvingen opgenomen van alle functies en rollen die aanwezig zijn binnen de beveiligingsorganisatie.

Verantwoordelijkheden & taken beveiligingsorganisatie	College B&W*	Directie*	Afdelings-managers*	FG*	CISO*	Informatie-beveiligings controller	Informatie Coördinator *	Privacy & Informatiebeveiliging beheerders, Security Officer Suwinet, Functionaris Rijbewijzen en Reisdocumenten	CISO Equalit*	Security Architect	PO Netwerk & Security	Interne Controle*
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	C	I		I	I			
Beheer van het register van verwerkingen	A	I	C	R				C				
Op basis van betrouwbaarheidseisen classificatie voor de eigen informatiesystemen vaststellen;		I	A	C	C	I	C	R	R			
Het uitvoeren van DPIA's en risicoanalyses		I	A	C	C	I	C	R	R			
De keuze en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen en DPIA's en risicoanalyses		I	A	C	C	I	C	R	R	C	C	
De implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen DPIA's en risicoanalyses		I	A	C	C	I	I	R	R	C	R	
Controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden				A/R	A/R			R	R			
Evalueren periodiek (strategische) beleidskaders en stellen deze waar nodig bij.				A/R	A/R							
Organisatie brede toetsing en auditing op naleving beveiligingsbeleid				A	A	C						R
Sturen op privacy en informatiebeveiligingsbewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn);	A	R	R	R	R	R	R	R	R			R
Rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.				A/R	A/R							
Coördinatie beveiligingsincidenten		I	C	A/R	A/R	I	C	R	R	C/I	C/I	
Het verzorgen van advies bij vragen uit de organisatie/ nieuwe projecten				A/R	A/R			R	R	C		

Tabel 1: RACI-matrix verantwoordelijkheden en taken beveiligingsorganisatie

3.2.2 Overlegstructuur

Nu alle verantwoordelijkheden en taken belegd zijn, is het belangrijk om ook praktische invulling te geven aan de beveiligingsorganisatie. Zoals al eerder genoemd fungeren de CISO en FG als overkoepelend aanspreekpunt en zijn zij verantwoordelijk voor het goed functioneren van de gehele beveiligingsorganisatie. Tijdens een maandelijks overleg met de directie, informatiecontroller en informatiecoördinator geven de CISO en FG een update over de werking van de beveiligingsorganisatie. Tijdens dit overleg wordt o.a. de status van risicoanalyses en DPIA's besproken, waar lopen we als beveiligingsorganisatie tegen aan en waar is input vanuit directie voor nodig.

Naast het maandelijkse overleg met directie, hebben de CISO en FG elk een eigen maandelijks overleg met de beveiligingsbeheerders. In dit overleg worden operationele zaken besproken, die binnen de vakafdelingen actueel zijn. Denk hierbij aan onderwerpen als het opstellen van beleidskaders, het uitvoeren van risicoanalyses, DPIA's, het opstellen van verwerkersovereenkomsten en bewustwording.

Om het informatiebeveiligingsoverleg en het privacyoverleg vorm te geven zijn er op een aantal sleutelplekken in de organisatie, beveiligingsrollen benoemd die decentraal bij de vakafdelingen werken. Dit betreft de functie van Security Officer Suwinet, Beveiligingsfunctionaris Reisdocumenten en Rijbewijzen, CISO Equalit en de privacybeheerders (voor taakbeschrijving zie bijlage 2). Omdat de bovengenoemde beveiligingsrollen nog niet alle sleutelposities afdekken, zullen er additioneel informatiebeveiligingsbeheerders worden aangewezen op de volgende posities:

- Facilitaire zaken;
- Inkoop;
- Functioneel Beheer;
- PIM;
- P&O;
- GEO (BAG, BGT, BRO);
- Sportbedrijf;
- Gemeentewerf.

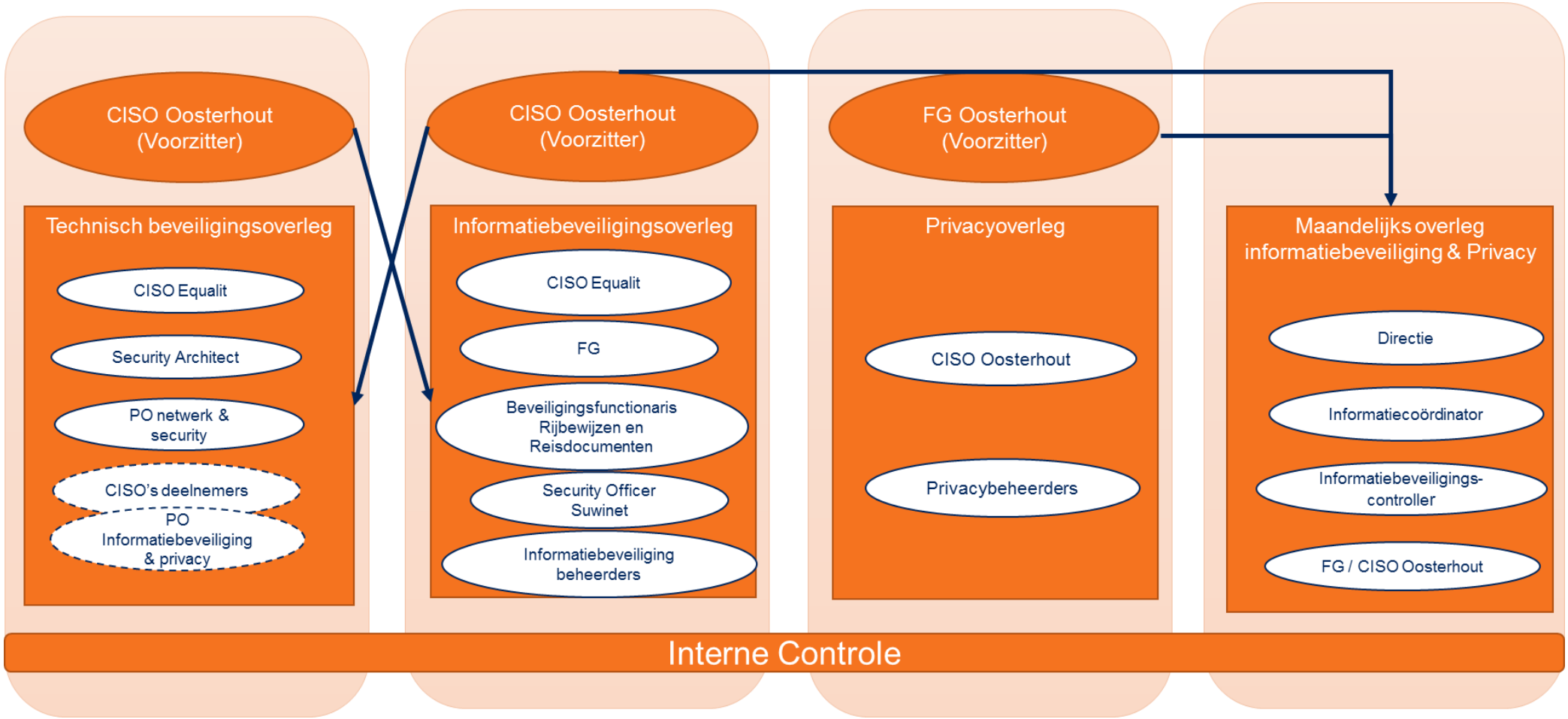
De bovenstaande informatiebeveiligingsbeheerders worden aangesteld naast de al reeds aangewezen privacybeheerders. Het informatiebeveiligingsoverleg en het privacyoverleg worden samengevoegd tot één overleg, waar de onderwerpen dit toelaten.

Tenslotte vormt de ICT-organisatie, Equalit, een belangrijk onderdeel van de beveiligingsorganisatie. Binnen Equalit zijn er een aantal security rollen benoemd, welke gezamenlijk bijdragen aan het ontwikkelen en actueel houden van de technische kant van de beveiliging. Security rollen binnen Equalit zijn:

- CISO Equalit;
- Security Architect;
- Product Owner Network & Operational Security;
- Security Specialist.

Om te zorgen voor een goede aansluiting tussen de technische en organisatorische aspecten van de beveiliging, vindt er een maandelijks technisch overleg plaats. Het technisch beveiligingsoverleg is een overleg binnen Equalit waarbij de CISO van Oosterhout aansluit om de verbinding en samenwerking op te zoeken. Het doel van het overleg is om elkaar te informeren, kennis uit te wisselen en plannen te volgen. Derhalve is er geen directe verantwoordingslijn voor de technisch specialisten aan de CISO van Oosterhout. Dit overleg zorgt er o.a. voor dat technische en organisatorische maatregelen op elkaar aansluiten. Waar noodzakelijk voor specifieke onderwerpen worden ook de CISO's van de andere Equalit gemeente uitgenodigd voor het technisch overleg.

In figuur 4 is een visuele weergave van de overlegstructuur weergeven.



Figuur 4: Overlegstructuur beveiligingsorganisatie

3.3 Samenhang beveiligingsbeleid en jaarplannen

Dit beveiligingsbeleid heeft een looptijd van drie jaar en biedt kaders voor het uitvoeren van risicoanalyses en opstellen van jaarplannen per beveiligingsonderdeel. Het beveiligingsbeleid wordt jaarlijks door middel van deelplannen op onderdelen geoperationaliseerd. Dit betekent dat de concrete uitvoering van dit beveiligingsbeleid door middel van het implementeren van beveiligingsmaatregelen plaatsvindt.

Naast een overkoepelend jaarplan voor informatiebeveiliging zijn er jaarplannen:

- BPR/PUN
- Suwinet
- Equalit

In de jaarplannen voor beveiliging worden, met behulp van de uitkomsten van de risicoanalyses, beschreven welke maatregelen geïmplementeerd moeten worden, maar ook welke maatregelen niet geïmplementeerd worden en waarom (pas toe of leg uit principe). Er wordt beschreven op welke manier de maatregelen geïmplementeerd moeten worden en door wie (planning).

De deelplannen worden opgesteld in samenwerking tussen de CISO, FG, Security Officer Suwinet, beveiligingsfunctionaris reisdocumenten en rijbewijzen en de informatiebeveiligingsbeheerders. Het concernoverleg stemt in met het plan vanuit de rol van het management als integraal verantwoordelijke voor de beveiliging van de afdeling. De directie stelt de deelplannen vast.

3.4 Rapporteren van beveiligingsincidenten

Ieder beveiligingsincident wordt gemeld bij de CISO of de FG. Indien het gaat om een datalek dan zorgt de FG voor melding van het datalek bij de Autoriteit Persoonsgegevens.

3.5 Benodigde middelen

Net zoals wanneer we ons privébezit beschermen kost ook het beschermen van de bedrijfsmiddelen van de gemeente geld. Privé maken we ook risicoafwegingen wanneer we ons verzekeren. Bijvoorbeeld: Hoe groot is de kans dat mijn fiets gestolen wordt en wat kost een verzekering mij?

Ondanks dat we zorgvuldig omgaan met het inschatten van risico’s en afwegen van kosten en baten, kost beveiliging gewoon geld. Deze kosten verdelen we in structurele kosten zoals personeelskosten voor beveiligingsbeheerders en kosten voor bewustwording en concernbrede technische en fysieke maatregelen.

Nieuw in deze structurele kosten zijn de uren die nodig zijn voor de aan te wijzen informatiebeveiligingsbeheerders.

Naast structurele jaarlijkse kosten, worden kosten gemaakt op basis van jaarlijks te bepalen incidentele maatregelen. Deze laatste worden, afhankelijk van het organisatieonderdeel of onderdelen waar de maatregelen betrekking op hebben, centraal of op afdelingsbudget begroot.

Ten slotte kunnen er ook incidentele kosten ontstaan in geval er bij plotseling optredende risico’s passende maatregelen genomen moeten worden.

4 Communicatie en bewustwording

4.1 Beveiliging is mensenwerk

Zoals eerder al gezegd: beveiliging is mensenwerk. Management en medewerkers dienen zich bewust te zijn van de risico's die samenhangen met de omgang met vertrouwelijke gegevens en van de noodzaak van beveiliging. Er kunnen voor de gemeente meerdere redenen zijn om te werken aan het verhogen van het kennis- en bewustzijnsniveau van de medewerkers. In de jaarlijkse uitvoeringsplannen wordt de focus, het primaire communicatiedoel, bepaald voor het betreffende jaar. Onderwerpen hierbij zijn:

- *Een streven naar kwaliteitsverbetering. Door het verhogen van het besef van de waarde van informatie voor de gemeente, houden gemeentelijke medewerkers zich beter aan procedures op dit gebied, waardoor het aantal fouten wordt verkleind.*
- *Het verkrijgen/behouden van een betrouwbaar imago. Voor de gemeente is vertrouwen één van de basisprincipes. Hierdoor is het van groot belang dat de gemeente betrouwbaar overkomt. Beveiligingsincidenten hebben een negatief effect op de betrouwbaarheid van de gemeente. Door een verhoging van het beveiligingsbewustzijn neemt het aantal beveiligingsincidenten af.*
- *De kracht van beveiliging wordt bepaald door een samenspel van technische en organisatorische factoren. Gedrag van mensen speelt hier bij een belangrijke rol. Het is daarom belangrijk dat de medewerkers van de gemeente Oosterhout zich bewust zijn van beveiliging. Het moet een natuurlijk onderdeel zijn van hun werk. Belangrijk hierbij is uiteraard dat mensen moeten worden geholpen bij het goed uitvoeren van beveiliging, bijvoorbeeld door het zorgen voor voldoende concrete richtlijnen.*

Er moeten een aantal randvoorwaarden ingevuld zijn om een effectieve en efficiënte invulling te kunnen geven op de vraag: 'Hoe kan het kennis- en bewustzijnsniveau van de medewerkers blijvend gestimuleerd, verhoogd en gestuurd worden op het gebied van beveiliging?' Deze randvoorwaarden zijn:

Commitment van de directie en het management
De cruciale voorwaarde voor een succesvolle uitvoering van een bewustwordingsprogramma binnen de gemeente Oosterhout is commitment. Zonder dat aan deze voorwaarde wordt voldaan is de slagingskans van een dergelijk programma beperkt.

Geen eenmalige exercitie
Bewustwording van gemeentelijke medewerkers binnen de gemeente is geen eenmalige zaak. Het is noodzakelijk dat er continu gestimuleerd, gestuurd en gemeten wordt. Zo wordt er constant aandacht besteed aan de ontwikkeling van het kennis- en bewustzijnsniveau. Hierbij is het wel van belang om vooraf het gewenste en het huidige kennis-, bewustzijnsniveau en gedrag in kaart te brengen. Tot slot dient het bewustwordingsprogramma ook aan te sluiten bij de organisatiecultuur van de gemeente Oosterhout.

4.2 Aanvullende kaders voor beveiliging

In dit beleidsplan zijn de uitgangspunten gegeven voor beveiliging in brede zin. Op onderdelen is aanvullend beleid nodig. Enerzijds vanuit wet- en regelgeving zoals bijvoorbeeld vanuit wet Suwi, wet BRP, PUN, BAG, BGT en BRO. Anderzijds is uitwerking nodig op specifieke onderdelen zoals bijvoorbeeld de fysieke beveiliging.

4.2.1 Aanvullende wettelijke kaders

Bij dit beveiligingsbeleid zijn aanvullende wettelijke kaders voor beveiliging van belang, waaronder Suwi, BRP en PUN. Deze beveiligingseisen voor deze wettelijke kaders zijn voor Oosterhout uitgewerkt in een tweetal beveiligingsplannen, namelijk:

- Beveiligingsplan Suwinet: dit plan beschrijft de wijze waarop de gemeente Oosterhout de beveiliging rondom Suwinet geregeld heeft.
- Beveiligingsplan BRP/PUN: dit plan beschrijft de wijze waarop de gemeente Oosterhout de beveiliging rondom de basisregistratie personen (BRP) en paspoorten en Nederlandse identiteitskaarten (PUN) geregeld heeft.

4.2.2 Aanvullende beleidsuitgangspunten

Als aanvulling op de strategische uitgangspunten in dit beleid, zijn er nog een aantal onderliggende beleidskaders en procedures nodig die een tactische en operationele invulling geven aan thema's binnen informatiebeveiliging en privacy. Een aantal onderwerpen waarvan de onderliggende beleidskaders direct relateren aan dit beveiligingsbeleid zijn:

- Dataclassificatie;
- Extern leveranciersmanagement;
- Identity & Access management (logische en fysieke toegangsbeveiliging)
- Cryptografische beheersmaatregelen;
- Patch & vulnerability management;
- Incidentmanagement;
- Bedrijfscontinuïteit.

4.3 Interne informatie – het intranet

Er is al veel informatie te vinden onder de button privacy en informatiebeveiliging op intranet. Op intranet is informatie te vinden over de volgende beveiligingsonderwerpen:

- Elektronisch gebruik communicatiemiddelen en gedragscode:
    - Telewerken;
    - Wachtwoordbeleid;
    - Clean/clear desk policy;
    - Aanvaardbaar gebruik bedrijfsmiddelen;
- Incidentmanagementprocedure (o.a. procedure datalekken);
- Verwerkingsregister;
- Sjabloon verwerkersovereenkomst;
- Rechten van betrokkenen;
- ENSIA;
- Beveiligingsbeleid;
- Bewustwording campagne: E-learning.

Bijlage 1: Begrippenlijst

- AP: Autoriteit persoonsgegevens
- AVG: Algemene verordening gegevensbescherming
- BAG: Basisregistratie Adressen en Gebouwen
- BGT: Basisregistratie Topgrafie
- BRO: Basisregistratie Ondergrond
- BIG: Baseline Informatiebeveiliging Gemeenten
- BIO: Baseline Informatiebeveiliging Overheid (vervangt BIG)
- BRP: Basisregistratie Personen
- CIP: Centrum voor Informatiebeveiliging en Privacy
- ENSIA: Eenduidige Normatiek Single Information Audit[5]
- IBD: Informatiebeveiligingsdienst VNG
- ISO 27001: ISO standaard voor informatiebeveiliging
- ISO 27002: ISO standaard voor informatiebeveiliging (best parctices)
- PUN: Persoons- en Identiteitskaarten Nederland
- Suwinet: Netwerk op basis van wet SUWI (structuur uitvoeringsorganisatie werk en inkomen)
- VNG: Vereniging Nederlandse Gemeenten

[5] https://www.ensia.nl/wat-is-ensia/#!/

Bijlage 2: Rol- en Functiebeschrijvingen beveiligingsorganisatie

Portefeuillehouder

- Integraal eindverantwoordelijk voor de beveiliging van informatie en bescherming van privacy in de gemeente;
- Opstellen van kaders o.b.v. organisatiedoelstellingen en wet & regelgeving;
- Beheer van het register van verwerkingen;
- Aanstellen CISO en FG;
- Raad informeren.

Gemeentesecretaris

- Integraal eindverantwoordelijk voor de beveiliging van informatie en bescherming van privacy binnen de organisatie;
- Opstellen van kaders o.b.v. organisatiedoelstellingen en wet & regelgeving;
- Sturen op privacy en informatiebeveiligingsbewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn).

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:

- Privacybeleid onderhouden;
- Risico's signaleren op het gebied van bescherming van persoonsgegevens;
- AVG uitleggen aan de organisatie;
- 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;

- Coördineren van Data Protection Impact Assessments (DPIA’s);
- Privacy werkzaamheden coördineren samen met de privacybeheerders;
- Ontwerpen toetsen en voorstellen doen vanuit het oogpunt van privacybescherming;
- Behandelen van vragen en klachten over de AVG van mensen binnen en buiten de organisatie;
- Zorgen voor bewustwording en het in stand houden van de bewustwording;
- 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.

Informatiebeveiligingscontroller

De informatiebeveiligingscontroller heeft de volgende taken:

- Goedkeuring ENSIA audit;
- Zorgen voor aansluiting met College B&W en de Raad;
- Zorgt voor opdrachtverstrekking richting auditor.

Informatiecoördinator

De informatiecoördinator heeft de volgende taken:

- Evalueren van beveiligingsincidenten;
- Namens de organisatie gemandateerd om informatie op te vragen bij alle gemeentelijke locaties;
- Bewaakt de integratie tussen 3 domeinen van informatiebeveiliging, privacy en informatiemanagement;
- Gaat over budget.

Beveiligingsbeheerders

Op een aantal sleutelplekken in de organisatie zijn beveiligingsrollen benoemd die decentraal bij de vakafdelingen werken. Dit betreft de functie van Security Officer Suwinet, Beveiligingsfunctionaris Reisdocumenten en Rijbewijzen, Product Owner Informatiebeveiliging & Privacy Equalit en de privacybeheerders.

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.

Informatiebeveiligingsbeheerders

De informatiebeveiligingsbeheerder is aanspreekpunt voor informatiebeveiliging binnen de afdeling en draagt bij aan de doorontwikkeling van informatiebeveiliging binnen zijn vakgebied. Taken van de informatiebeveiligingsbeheerder 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 het ENSIA verantwoordingsproces binnen het eigen vakgebied;
- Het bieden van ondersteuning bij het classificeren van informatiesystemen;
- In overleg met de CISO de organisatie begeleiden en 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;
- Het verstrekken van advies en het opstellen van een rapport bij een beveiligingsincident;
- Toetsing van afdelings-, cluster- of unitplannen op het gebied van informatiebeveiliging.

Privacybeheerders

De privacybeheerder heeft een belangrijke rol op de werkvloer met betrekking tot het thema privacy. De privacybeheerder informeert en adviseert de afdeling over privacy en bescherming van persoonsgegevens. Denk daarbij aan:

- 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?

Daarnaast draagt de privacybeheerder bij aan de doorontwikkeling van privacy binnen de afdeling. Dit gebeurd onder andere door, in overleg met de FG (functionaris gegevensbescherming), de afdeling te begeleiden bij en helpen met het verder toepassen en implementeren van termen als ‘privacy by design’ en ‘privacy by default’.

Taken voor de privacybeheerder

- Het uitvoeren (projectleider) van een DPIA;
- Inhoudelijke en procedurele ondersteuning van de eigenaar bij het doorlopen van de DPIA;

- Opstellen rapport inclusief maatregelen DPIA;
- Coördinatie van de actualisatie van het register van verwerkingen;
- Het opstellen en controleren van de verwerkersovereenkomsten van de afdeling;
- Adviseren m.b.t verwerkersovereenkomst;
- Inventariseren van de feiten en omstandigheden van een beveiligingsincident;
- Opstellen verslag beveiligingsincident;
- Verstrekken van advies bij een beveiligingsincident;
- Opstellen en versturen rapportage veiligheidsincident beveiligingsincident;
- Gevraagd en ongevraagd advies verlenen aan bestuur, management en medewerkers m.b.t. privacyvraagstukken;
- Voorlichting en communicatie over privacy (bewustwording) aan de afdeling;
- Procedureel en inhoudelijk ondersteunen bij de procedure verzoek rechten van betrokkenen persoonsgegevens;
- Verzoeken m.b.t. rechten van betrokkenen uitvoeren.

Interne Controle

Interne controle heeft de volgende taken:

- Organisatie brede toetsing en auditing op naleving beveiligingsbeleid;
- Auditplan vaststellen;
- Verzamelen bewijslast;
- Opvolging uitgezette acties ten behoeve van implementatie maatregelen.

Security rollen Equalit

Een belangrijk onderdeel van de beveiligingsorganisatie is de ICT-organisatie, Equalit. Binnen Equalit zijn er een aantal security rollen benoemd welke gezamenlijk bijdragen aan het ontwikkelen en actueel houden van informatiebeveiliging binnen de ICT-organisatie. Security rollen die je bij Equalit vindt zijn:

- CISO Equalit;
- Security Architect;
- Product Owner Network & Operational Security;
- Security Specialist.

CISO Equalit

De CISO Equalit heeft de volgende taken:

- Het vertalen van het informatiebeveiligingsbeleid Oosterhout naar passende (technische) maatregelen voor Equalit;
- Zorgdragen voor het vereiste niveau van informatiebeveiliging binnen Equalit om te voldoen aan gestelde wet- en regelgeving;
- Controleren op de juiste uitvoering van het informatiebeveiligingsbeleid binnen Equalit;
- 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 BIG om te voldoen aan de diverse audit.

Security Architect

De Security Architect heeft de volgende taken:

- Vertaalt beleidskaders voor informatiebeveiliging en privacy naar ICT-architecturen en vervult daarbij zowel een architect- als adviseursrol;
- Ontwikkelt en houdt de aspecten informatiebeveiliging en privacy binnen de ICT-architectuur actueel;
- Treedt met name op als ICT-architect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging- en auditing;
- Toetst ICT-ontwerpen aan architectuurprincipes voor beveiliging en adviseert indien nodig over verbetering van die ontwerpen;
- Houdt voortdurend zicht op marktontwikkelingen op het gebied van informatiebeveiligingsproducten.

Product Owner Network & Operational Security

De Product Owner Network & Operational Security (NOS) is verantwoordelijk voor de implementatie en doorontwikkeling van diensten op het gebied van netwerken en operational security. De Product Owner werkt samen met het NOS team en heeft veel contact met stakeholders. De Product Owner Network & Operational Security heeft de volgende taken**:**

- Het beheren van de product backlog van het NOS team en zorgen dat alle zaken op de backlog duidelijk zijn omschreven en zijn geordend op de waarde die ze toevoegen;
- Het opstellen van een roadmap en visie samen met de stakeholders, waaronder architecten en CISO's;
- Het accepteren van de door het CISO team opgeleverde producten en bepalen wanneer deze in productie worden genomen;
- Het continue op de hoogte blijven van ontwikkelingen binnen je vakgebied om te zorgen dat de backlog, roadmap blijven aansluiten bij ontwikkelingen op het gebied van bijvoorbeeld wet- en regelgeving;
- Afstemming met leveranciers;
- Het beheren van het problem management proces en periodiek rapporteren hierover;
- Komen met verbetervoorstellen m.b.t. de eigen afdeling en Operations in het algemeen;
- Opstellen van rapportages en borgen van documentatie en richtlijnen.

Security Specialist

De Security Specialist is verantwoordelijk voor de operationele security binnen de organisatie. De Security specialist is verantwoordelijk voor het voorkomen, detecteren en oplossen van security incidenten en helpt met het uitdenken, implementeren en beheren van security diensten en producten. De Security Specialist maakt onderdeel uit van het Network & Operational Security (NOS) team. De Security Specialist heeft de volgende taken:

- Monitoren van de infrastructuur ter detectie van beveiligingsincidenten;
- Implementatie en beheer van security producten zoals antivirus, firewalls, IDS/IPS, mailbeveiliging;
- Incident response: onderzoeken, oplossen en voorkomen van security incidenten;
- Evaluatie van de huidige security d.m.v. vulnerability scans en penetratietests;
- Adviseren en ondersteunen van collega's op gebied van technische informatiebeveiliging;
- Bijhouden van ontwikkelingen op gebied van informatiebeveiliging.