gemeente Roermond

# GEMEENTEBLAD

Officiële uitgave van de gemeente Roermond

Nr. 25227

16 januari

2024

## Informatiebeveiligingsbeleid Roermond

Het college van burgemeester en wethouders van de gemeente Roermond heeft besloten het Informatiebeveiligingsbeleid Roermond vast te stellen.

**Inleiding**

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging voor de gemeente Roermond. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Dit beleid is gebaseerd op de norm 'Baseline Informatiebeveiliging Overheid (BIO)'.
De BIO is van toepassing op de overheid en hiermee op de volgende bestuursorganen:

- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

In dit document is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteitshandhaving van de) bedrijfsvoering.

**Informatiebeveiliging**
Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk verrassingen met negatieve gevolgen voor de bedrijfsvoering, waarbij het bereiken van de gestelde doelen in gevaar wordt gebracht. Het begrip 'informatiebeveiliging' heeft betrekking op:

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

**Waarom informatiebeveiliging?**
Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor de gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan inwoners en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

**Reikwijdte en afbakening informatiebeveiliging**
Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm, smartphone, tablets, et cetera) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk en clear screen policy implementeren of hoe om te gaan met mobiele apparatuur en aanwijzingen voor telewerken.

Informatiebeveiliging vormt een onderdeel van de kwaliteitszorg voor bedrijfsprocessen en ondersteunende informatiesystemen en richt zich op de beschikbaarheid, vertrouwelijkheid en integriteit van de geautomatiseerde informatievoorziening. Informatiebeveiliging is een lijnverantwoordelijkheid en onderdeel van de kwaliteitszorg voor organisatie- en bestuursprocessen en de ondersteunende informatiesystemen.

**Informatiebeveiligingsbeleid van de gemeente Roermond**

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

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door college van burgemeester en wethouders. Hiermee komt het oude Informatiebeveiligingsbeleid van de gemeente Roermond te vervallen.

## 1. Uitgangspunten informatiebeveiliging

### 1.1 Inleiding

***De belangrijkste uitgangspunten voor dit beleid zijn:***

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van burgemeester en wethouders is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het clustermanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Roermond hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, Do, Check en Act' (PDCA) vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde verwerking (zoals toegang, gebruik, verandering, openbaring, vernietiging, verlies, overdracht enzovoort) en bij vermeende inbreuken hiervan melding te maken bij servicedesk van ICT-NML.

***Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:***

- Het college van burgemeester en wethouders stelt als bestuurlijk verantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De Gemeentesecretaris en het Concern Management Team zijn ambtelijk verantwoordelijk voor het strategisch informatiebeveiligingsbeleid.
- Het Concern Management Team stelt jaarlijks het informatiebeveiligingsplan vast.
- Het Concern Management Team is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het Concern Management Team is verantwoordelijk voor het vragen om informatie bij de proceseigenaren en ziet erop toe dat de proceseigenaren adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hen verantwoording valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het Concern Management Team, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging naar aanleiding van de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De proceseigenaren zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, BAG, BGT en BRO) en toekomstige basisregistraties, het proces rond de aanvraag en uitgifte van paspoorten en Nederlandse identiteitskaarten (PNIK), het informatiesysteem rondom Suwinet allemaal belangrijk zijn in kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente.

Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die we gesteld hebben.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Proceseigenaren dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Proceseigenaren voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico afwegingen te kunnen maken.

**1.2 Het belang van informatie(veiligheid)**
Informatie is één van de voornaamste bedrijfsmiddelen van Roermond. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor inwoners, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

**Visie**

De gemeente Roermond zet in op een integraal risico gebaseerde informatiebeveiliging die een hoge mate van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie nastreeft.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. [1]

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

**1.4 Risicobenadering**
De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Roermond is risico gebaseerd. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de baseline. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact**.

**1.5 Doelgroepen**
Dit informatiebeveiligingsbeleid geldt voor de gemeente met de daaronder vallende diensten en kan ook (deels) worden opgelegd aan externe leveranciers of instanties waar mee samengewerkt wordt. De gemeente als opdrachtgever / systeemeigenaar is altijd verantwoordelijk voor de kwaliteit en veilig-

1) Medewerker = (1) ambtenaar in de zin van het Ambtenarenwet of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een organisatie verricht.

heid van de uitbestede diensten. De gemeente eist van de externe leveranciers dat zij voldoen aan alle aspecten van het Informatiebeveiligingsbeleid die voor de dienst of het betreffende systeem van belang zijn en betrekking hebben op de geleverde dienst. Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een verwerkersovereenkomst (zie artikel 28, lid 3 van de AVG[2]) afgesloten.

| Doelgroep | Relevantie voor Informatiebeveiligingsbeleid |
|---|---|
| College van burgemeester en wethouders | Integrale eindverantwoordelijkheid |
| Gemeentesecretaris / Algemeen directeur | Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de Gemeentesecretaris/Algemeen directeur verantwoordelijk voor de uitvoering van organisatie brede vraagstukken ten aanzien van informatiebeveiliging. |
| Concern Managent Team (CMT) | Kaderstelling en implementatie |
| Cluster- en Opgavemanagers | Planvorming binnen de informatiebeveiligingskaders |
| Alle leidinggevenden | Sturing op informatieveiligheid en controle op naleving |
| Proceseigenaar | De proceseigenaar is de persoon die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem. Classificatie: bepalen van beschermingseisen van informatie |
| Alle medewerkers | Gedrag en naleving |
| CISO | Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid |
| Cluster Bedrijfsvoering | Arbeidsvoorwaardelijke zaken |
| Cluster Beheer vastgoed | Fysieke toegangsbeveiliging |
| ICT NML | ICT-beheer, ICT-onderhoud en Technische beveiliging |
| Auditors | Onafhankelijke toetsing van het beleid |
| Leveranciers en ketenpartners | Compliance aan het beleid |
| Dienstenleverancier | Bedoeld wordt de dienstenleverancier (bijv. SSC) binnen de overheid of organisaties in de markt waaraan de Gemeentesecretaris/Algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak in-besteedt respectievelijk uitbesteedt. |

### 1.6 Scope

- De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
- Dit informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[3]
- Gemeenten zijn de afgelopen jaren voornamelijk aan de slag gegaan met het beschermen van informatie door middel van de implementatie van de Baseline Informatiebeveiliging voor de Overheid (BIO). De BIO implementatie is gericht op bescherming van informatie in de ICT van de gemeente, waar de nadruk ligt op bescherming van vertrouwelijkheid. Gemeenten gebruiken ook automatisering voor besturing van industriële toepassingen, hierbij kun je denken aan besturing van bruggen en sluizen, verkeerslichten, maar ook gebouwbeheerssystemen. Deze industriële automatisering wordt ook wel OT (operationele technologie) of PA (procesautomatisering) genoemd.
  Traditioneel communiceerden PA-systemen rechtstreeks met elkaar in een gesloten netwerk, ze waren niet gekoppeld aan het internet of andere netwerken. Tegenwoordig wordt steeds vaker een netwerkcomponent ingebouwd zodat beheer op afstand mogelijk wordt. Daarnaast is er ook een beweging gaande om sensor- en besturingstechniek in te zetten voor het meten, regelen en

2) Sinds 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Deze verordening zorgt ervoor dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt sinds die datum niet meer.

3) Bijvoorbeeld Wet SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

besturen van dingen in de publieke ruimte, dit wordt ook wel aangeduid met de term IoT (Internet of Things) en smart city concepten. Daarvoor worden ook steeds vaker koppelingen tot stand gebracht met de ICT-omgeving van de gemeente. De nadruk op de bescherming van PA en IoT ligt op veiligheid (safety), integriteit en beschikbaarheid, de beveiligingsfocus is dus anders dan bij ICT-systemen.

Hiervoor dient een apart PA-beleid opgesteld te worden. De VNG biedt hiervoor een handreiking aan.

**1.7 Informatiebeveiligingsbeleid en architectuur**

- Informatiebeveiliging is onderdeel van de informatiearchitectuur en zal worden uitgewerkt als onderdeel van die architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).[4]

**1.8 Relevante wet- en regelgeving**

**Doelstelling**

De gemeente Roermond hanteert de volgende doelstellingen:

- Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

**Implementatie**

Er is in dit document vastgesteld welke wetten en wettelijke maatregelen van toepassing zijn op de informatiebeveiliging van de gemeente Roermond.

**Juridische grondslag**

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Algemene verordening gegevensbescherming (AVG).
Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De AVG regelt in artikel 5 en 32 welke maatregelen organisaties moeten treffen, in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft de gemeente is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 9 en 10 AVG en artikel 22 t/m 31 van de Uitvoeringswet AVG. Deze maatregelen maken deel uit van het ISMS van de gemeente Roermond.

**Bepaalde wetten nader toegelicht**

- De Wet BRP is met ingang van 6-1-2014 het wettelijke kader waaraan alle betrokkenen bij de basisregistratie van persoonsgegevens zich moeten houden. Om de kwaliteit van de Basisregistratie personen te waarborgen heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) in Artikel 4.3 van de Wet BRP vastgelegd op welke manier periodiek onderzoek verricht moet worden naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie, voor zover het de gemeentelijke voorziening betreft of het college van burgemeester en wethouders verantwoordelijk is voor de bijhouding. Op basis van dit artikel dient er ook periodiek gerapporteerd te worden aan het Autoriteit Persoonsgegevens (AP) en aan De Minister van het ministerie van BZK.
- Op basis van artikel 94 van de Paspoortuitvoeringsregeling Nederland 2001 worden er eisen gesteld aan de beveiliging van informatie en de rapportage hierover. Op basis van dit artikel dient er een controle te worden uitgevoerd op de toepassing van de beveiligingsmaatregelen.
- Artikel 59 van de Paspoortwet stelt nadere regels met betrekking tot de uitvoering van deze wet, de door de betrokkene in het kader van het aanvraag- en uitgifteproces van reisdocumenten over te leggen gegevens en de beoordeling daarvan, alsmede de beveiliging van dit proces.
- Daarnaast dient iedere gemeente vanaf 2004, overeenkomstig artikel 6.4, Regeling SUWI, in een beveiligingsplan aan te geven op welke wijze zij invulling geeft aan de beveiliging van de gegevensuitwisseling in het kader van SUWI. Ook moet de gemeente voldoen aan de beveiligingseisen, die als Suwinet partij aan de gemeente worden gesteld.
- In 2012 zijn de ICT-Beveiligingsrichtlijnen voor webapplicaties van kracht geworden. Deze richtlijnen zijn in 2015 herzien. De ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC) vormen een leidraad voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. De Beveiligingsrichtlijnen zijn breed toepasbaar voor ICT- oplossingen die gebruikmaken van webapplicaties. Hierdoor zijn ze zowel door afnemers,

4) De processen van informatiebeveiliging worden onderdeel van de volgende GEMMA versie om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.

als door dienstaanbieders te gebruiken voor aan- en uitbestedingen, toezicht en onderlinge afspraken.
- Op basis van de Archiefwet dient de gemeente de nodige maatregelen te treffen om het risico op beschadiging of het verloren gaan van het papieren archief te voorkomen of te beperken.

**Relevante wet en regelgeving**

Wetten en regelingen die van toepassing zijn (niet limitatief):

- Algemene verordening gegevensbescherming (AVG) ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR)
- Algemene wet bestuursrecht
- Ambtenarenwet
- Archiefbesluit (AB) 1995 (in navolging van de Archiefwet (AW) 1995)
- Archiefregeling 2010
- Archiefverordening gemeente Roermond van 6-6-2019
- Archiefwet
- Auteurswet
- Baseline Informatiebeveiliging Overheid (BIO)
- Besluit Begroten en Verantwoorden (BBV) uit 2003
- Beheerregeling Informatiebeheer Roermond 2019
- CAO gemeenten
- ISO 27001:2017 en ISO 27002:2017
- Comptabiliteitswet
- GIBIT - Gemeentelijke inkoopvoorwaarden bij IT, versie van november 2020
- Jeugdwet
- Participatiewet
- Paspoortwet en Paspoortuitvoeringsregeling Nederland 2001 (PUN)
- Programma van Eisen PKI Overheid
- RAGR (Regeling Arbeidsvoorwaarden Gemeente Roermond)
- Registratiewet
- Richtlijnen van het nationale Cyber Security Center (NCSC) en de Informatiebeveiligingsdienst voor gemeenten (IBD), een onderdeel van VNG Realisatie
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Uitgangspunten online communicatie rijksambtenaren
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)
- Wet BAG
- Wet BRO
- Wet BRP
- Wet Computercriminaliteit III
- Wet Eenmalige Gegevens uitvraag (WEU)
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet Maatschappelijke Ondersteuning (WMO)
- Wet Meldplicht datalekken
- Wet op de identificatieplicht
- Wet open overheid (Woo)
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (Wpbr)
- Wet Politiegegevens (WPG)
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)
- Wet Veiligheidsonderzoeken (WVO)

## 2. Organisatie van de informatiebeveiliging

### 2.1 Inleiding

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende '*Three Lines of Defence*' (3LoD), beschreven in de 'Strategie Interne Beheersing' die op 18 april 2023 door het college is vastgesteld. In dit model is het lijnmanagement (clusters-, opgave- en/of concernmanagers) verantwoordelijk voor de eigen processen.
De tweede lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

**2.2 Aansturing: Concern Management Team (CMT)**
Het Concern Management Team (CMT) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een proceseigenaar. Het CMT zorgt dat de proceseigenaren zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het CMT zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college van burgemeester en wethouders gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering.

Het CMT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het CMT draagt zorg voor het uitwerken van tactische informatiebeveiliging beleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het CMT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Roermond gezien als een integraal onderdeel van Risicomanagement.

**2.3 Uitvoering: Proceseigenaren**
Informatiebeveiliging valt onder de verantwoordelijkheden van alle proceseigenaren en om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben, er moet dus altijd iemand verantwoordelijk zijn. Proceseigenaren rapporteren over de door hun tactisch- en operationeel uitgevoerde informatiebeveiliging activiteiten aan het Concern Management Team. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de proceseigenaren in het kader van informatiebeveiliging zijn het:

1. leveren van input voor wijzigingen op maatregelen en procedures;
2. binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures;
3. vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
4. bespreken van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen. Voorbereiding en coördinatie van het overleg ligt bij de CISO.

**2.4 Controle en verantwoording**
Dit beleid is een verantwoordelijkheid van het bestuur van de gemeente. De bestuurders en het Concern Management Team van de gemeente Roermond zullen richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
Het Concern Management Team is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het Concern Management Team rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit beleid.

**2.5 Verantwoording: ENSIA**
De gemeente verantwoordt zich jaarlijks over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks de interne ENSIA-coördinator ervoor zorgt dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren. De proceseigenaren leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

ENSIA staat voor Eenduidige Normatiek Single Information Audit en met ENSIA verantwoordt de gemeente zich jaarlijks ook horizontaal aan de gemeenteraad. Het verantwoordingsproces over informatieveiligheid bij gemeenten wordt hiermee verder geprofessionaliseerd door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de Collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van burgemeester en wethouders aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de Collegeverklaring aan de Raad.

Middels deze verantwoording wordt het bestuur van de gemeente Roermond en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente Roermond

informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

**2.6 Taken en rollen**

- **Het college van burgemeester en wethouders** stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het college van burgemeester en wethouders als de gemeenteraad (control functie) kunnen hiervoor opdracht geven om dit te (laten) controleren. Het Concern Management Team adviseert het college van burgemeester en wethouders formeel over vast te stellen beleid.
- **De gemeentesecretaris / Algemeen directeur** geeft namens het Concern Management Team op dagelijkse basis invulling aan de sturende rol door besluitvorming in het Concern Management Team voor te bereiden en toe te zien op de uitvoering ervan. De taken m.b.t. informatiebeveiliging die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer'. De CISO bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per jaar organisatie breed aan het Concern Management Team over de stand van zaken. De gemeentesecretaris / Algemeen directeur draagt zorg voor onderstaande punten en wordt hierbij ondersteund door de CISO:
  - Het opstellen en onderhouden van Informatiebeveiligingsplannen, voor de informatiesystemen en verantwoordelijkheidsgebieden waarvoor de leidinggeveneden verantwoordelijk zijn.
  - Het uitvoeren en periodiek evalueren van de uit deze Informatiebeveiligingsplannen voortvloeiende maatregelen.
  - Het maken van schriftelijke afspraken met derden over het vereiste betrouwbaarheidsniveau en de wijze van toezicht hier op houden.
  - Het bijhouden van de onder deze verantwoordelijkheid vallende complete en actuele lijst van verantwoordelijkheidsgebieden en daaronder vallende informatiesystemen en procesautomatiseringsystemen.
  - Het zorgdragen dat de tot de gemeentelijke organisatie behorende medewerkers zorgvuldig met gegevens omgaan en zich bewust zijn van het risico dat daarbij wordt gelopen.
  - Het afhandelen van en periodiek rapporteren over binnengekomen meldingen van incidenten.
  - Rapporteert over de implementatie van de maatregelen in de management rapportages.
  - Rapporteert jaarlijks aan het Concern Management Team en aan het college van burgemeester en wethouders over het informatiebeveiligingsbeleid.

- **Gemeentearchivaris**:
  - De archivaris is wettelijk (artikels 32 en 37 Archiefwet 1995) verantwoordelijk voor het toezicht op het beheer van de archiefbescheiden, ongeacht hun vorm, welke nog niet zijn overgebracht naar de archiefbewaarplaats.
  - Houdt ook toezicht bij de betreffende archieven van gemeenschappelijke regelingen.
  - Rapporteert hierover jaarlijks aan het college van burgemeester en wethouders en aan de Raad conform art. 32, lid 2 van de Archiefwet 1995.

- **Concerncontroller**:
  - De concerncontroller toetst periodiek of uitvoering, naleving en controle conform afspraken/richtlijnen heeft plaatsgevonden en rapporteert aan het CMT.
  - Neemt de interne audits op in het Jaarplan Interne Audits Gemeente Roermond met als doel een betere beheersing van processen rondom informatiebeveiliging en het borgen van deze processen.

- **Chief Information Security Officer (CISO)**
  - Ten aanzien van het aspect Informatiebeveiliging vervult deze functionaris een bijzondere rol bij het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's.
  - Rapporteert rechtstreeks aan de gemeentesecretaris / algemeen directeur en de portefeuillehouder ICT.
  - Bevordert en adviseert gevraagd en ongevraagd over de beveiliging van de gemeente, verzorgt rapportages over de status, controleert of m.b.t. de beveiliging van de gemeente de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente en op het gebied van wet- en regelgeving:
    - Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi);
    - Basisregistratie Personen (Wet BRP);
    - Paspoortuitvoeringsregeling Nederland (PUN);

        - Het gebruik van DigiD (Digitale identiteit);

    - Begeleiden van in- en externe audits op die onderdelen waar deze de informatiebeveiliging raken.

- **Information Security Officer (ISO)**
    - De Information Security Officer vervult samen met de CISO een belangrijke rol in het opstellen van en vertalen van het informatiebeveiligingsbeleid naar (technische) beveiligingsmaatregelen. De Information Security Officer:
        - brengt continu de noodzaak van informatiebeveiliging bij de gemeente Roermond onder de aandacht;
        - adviseert de organisatie over te nemen beveiligingsmaatregelen waarbij de juiste vertaling wordt gemaakt naar bestuur, directie, management en medewerkers;
        - draagt zorg voor het vereiste niveau van informatiebeveiliging voor de audits en de coördinatie en uitvoering hiervan, zoals de audit vanuit ENSIA;
        - creëert bewustwording en zit daarvoor bij de afdelingen aan tafel en verzorgt presentaties voor diverse groepen (bijvoorbeeld medewerkers, directie, college).

- **Functionaris Gegevensbescherming (FG)**
    - De FG is de interne toezichthouder op de verwerking van de persoonsgegevens.
    - De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
    - De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.
    - Organisatie breed adviseren over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
    - Aanwijzingen geven aan gebruikers van systemen met betrekking tot persoonsregistraties.
    - Ongevraagd advies uit te brengen over alle producten die betrekking hebben op de registratie van personen.
    - Contactpersoon van de gemeente voor de Autoriteit Persoonsgegevens (AP).
    - Alle betrokkenen van wie persoonsgegevens verwerkt worden, zoals klanten en personeelsleden, kunnen bij een FG terecht voor informatie over en inzage in de eigen verwerkte persoonsgegevens of voor klachten.

- **Privacy Officer (PO)**
    - Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de PO (ook wel juridisch adviseur privacy), die in dit geval geen FG is, verantwoordelijk voor:
        - het vormgeven en bewaken van het privacybeleid binnen de gemeente;
        - ondersteunen bij het in kaart brengen van de risico's door bijvoorbeeld een Privacy Impact Assessment (PIA) uit te voeren;
        - op basis van het privacybeleid en de PIA's opstellen van een implementatieplan;
        - een adviserende rol richting de vakafdelingen en kan hij of zij vragen beantwoorden zoals:
        - hoe moeten we deze gegevens delen;
        - aan welke regels dienen we ons te houden;
        - welke maatregelen moeten we de externe partij opleggen.

- **Adviseur Informatiemanagement**
    - Toetst en evalueert de naleving van het Informatiebeveiligingsbeleid bij vraagstukken op meerdere samenhangende vakgebieden.

- **Adviseur Informatiebeveiliging en ICT**
    - Vervult een rol in het vertalen van het informatiebeveiligingsbeleid en informatiebeveiligingsplan naar technische en organisatorische beveiligingsmaatregelen;
    - brengt continu de noodzaak van informatiebeveiliging bij de gemeente Roermond onder de aandacht;
    - adviseert gevraagd en ongevraagd de organisatie over te nemen beveiligingsmaatregelen waarbij de juiste vertaling wordt gemaakt naar bestuur, directie, management en medewerkers;
    - creëert bewustwording en zit daarvoor bij de clusters en opgave teams aan tafel en verzorgt in samenwerking met de CISO en ISO presentaties voor diverse groepen (bijvoorbeeld medewerkers, directie, college).

- **Adviseur centrale gegevensvoorziening**

- Zorgt dat het Informatiebeveiligingsbeleid wordt nageleefd bij het koppelen van verschillende informatiesystemen.
- Adviseert gevraagd en ongevraagd proceseigenaren over de voorwaarden waaraan het uitwisselen van informatie tussen informatiesystemen dient te voldoen.

- **De beveiligingsbeheerder**
  Deze rol geldt ten aanzien van de specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel beveiligingsfunctionaris reisdocumenten), Rijbewijzen (officieel beveiligingsfunctionaris Rijbewijzen), BAG, SUWI (officieel Security officer SUWI) en DigiD.

  Gelet op artikel 2 van de Verordening gegevensverstrekking basisregistratie personen Roermond, de artikelen 1.10 en 1.11 van de Wet basisregistratie personen en artikel 6 van het Besluit basisregistratie personen is het wenselijk de hoofdlijnen van het beheer van de gemeentelijke basisregistratie personen in een regeling vast te leggen en door het college van burgemeester en wethouders te laten vastleggen.
- **Applicatiebeheer, onder verantwoordelijkheid van de clustermanager, heeft als taak**:
  - het informatiebeveiligingsbeleid binnen de aan hen toevertrouwde bedrijfsapplicaties te realiseren;
  - beheer van de applicaties;
  - beheer toegangsrechten gebruikers en wachtwoorden;
  - verantwoordelijk zijn voor goed functioneren applicatie;
  - bewaking van integriteit gegevens in applicatie;
  - herstel van gegevens na restore;
  - overleg met systeembeheer bij back-up met foutmelding of restore.

- **Elke medewerker**:
  - gaat op een bewuste manier om met gegevens en het verzamelen, vastleggen, verwerken en verstrekken van informatie (inclusief zijn werkplek) zoals vastgelegd in de procedures en voorschriften.
  - dient kennis te hebben van de gevolgen van zijn/haar gedrag op beveiliging.
  - meldt incidenten volgens de daartoe geëigende procedures aan de ICT Helpdesk. Meldingen die van vertrouwelijke aard zijn worden gemeld bij het verantwoordelijke afdelingshoofd.

- **ICT-beheerorganisatie (ICT NML)**:
  De ICT-beheerorganisatie heeft een security functionaris aangesteld voor dagelijks beheer van technische IB-aspecten. De security functionaris rapporteert aan de CISO van de gemeente Roermond. Informatiebeveiliging is onderdeel van de servicemanagement rapportage.

| **Wie** | **Plan:**<br>**Kaderstelling** | **Do:**<br>**Uitvoering** | **Check:**<br>**Controle** | **Act:**<br>**Verbetering** |
|---|---|---|---|---|
| Sturen:<br>Directie dagelijkse uitvoering: CISO | Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning. | Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons. | Controle, audit, pentesten. | Bijsturen:<br>Opdrachtverstrekking voor verbeteracties. Rapportage aan DT / B&W |
| Vragen:<br>Alle afdelingen | Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen. | Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management | Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy. | Verbeteren bedrijfscontinuïteit. Rapportage aan CIO/CISO |
| Uitvoeren:<br>Service organisatie<br>(in uitvoerende rol) | Beleidsvoorbereiding, technische onderzoeken (marktverkenningen). | Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies. | Vulnerability scanning, evaluatie en rapportage. | Uitvoeren verbeteracties. Advies aan de CIO/CISO over aanpassingen aan |

| | | | | |
|---|---|---|---|---|
| | | | | de informatievoorziening. |

**2.7 Afstemmingsoverleg**
Er dient afstemmingsoverleg informatiebeveiliging en privacy te zijn, waarin de verantwoordelijken voor fysieke beveiliging, Informatiebeveiliging, privacy en persoonlijke integriteit participeren. Dit heeft als doel te komen tot een integraal informatiebeveiligingsbeleid en de uitvoering daarvan. Daartoe wordt onderling de werkwijze, de werkzaamheden, jaarrapportages en te treffen maatregelen op het gebied van beveiliging afgestemd.
Het onderwerp Informatiebeveiliging dient periodiek een onderdeel te zijn op de agenda van het Concern Management Team zodat er sturing kan plaatsvinden op de uitgevoerde activiteiten.

**Maandelijks overleg met de gemeentesecretaris**

- Gemeentesecretaris (voorzitter)
- CISO (secretaris)
- Concerncontroller
- Information Security Officer (ISO)
- Privacy Officer (PO)
- Functionaris voor de Gegevensbescherming ((FG) - op afroep of op eigen initiatief zal de FG deelnemen aan het overleg).

**Maandelijks overleg met de portefeuillehouder Informatie en communicatietechnologie**

- Portefeuillehouder Informatie- en communicatietechnologie (voorzitter)
- CISO (secretaris)
- Information Security Officer (ISO)
- Privacy Officer (PO)
- Functionaris voor de Gegevensbescherming ((FG) - op afroep of op eigen initiatief zal de FG deelnemen aan het overleg).

**Een 3-wekelijks overleg van het team Informatiebeveiliging en privacy met Concernmanager**

- Concernmanager (voorzitter)
- Privacy Officer (PO)
- Functionaris voor de Gegevensbescherming ((FG)
- CISO
- Concern Controller
- Information Security Officer (ISO)
- Strategisch adviseur Informatiemanagement

**Wekelijks overleg Informatiebeveiliging en privacy**

- CISO (voorzitter)
- Privacy Officer (PO)
- Functionaris voor de Gegevensbescherming ((FG)
- Concern Controller
- Information Security Officer (ISO).
- Adviseur Informatiebeveiliging

**2.8 Externe partijen**
Informatiebeveiligingsbeleid, landelijke normen en wet- en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).[5]

Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV dienen te worden getoetst aan Informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of verwerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.[6]

5) Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Overheid.
6) Hiervoor kan gebruik worden gemaakt van een 'third party mededeling' (TPM), ISO27001 of een ISAE 3402-verklaring.

Voor het tot stand brengen van datakoppelingen met externe partijen, gelden naast dit generiek informatiebeveiligingsbeleid specifieke procedures. Het doel van deze procedures is risicobeheersing. Voor externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing.[7]

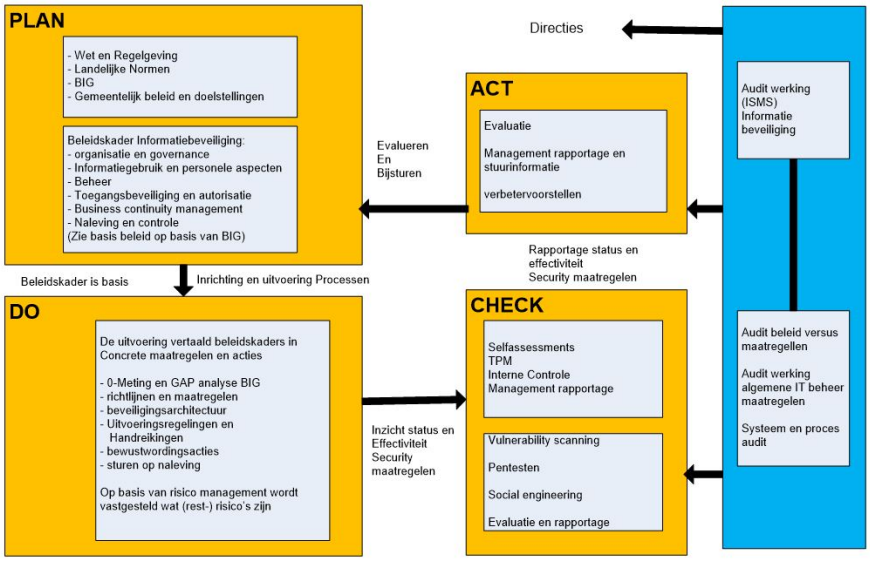
- De gemeente is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door externe partijen;
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;[8]
  - melding bij de Autoriteit Persoonsgegevens bij uitbesteding van het verwerken van persoonsgegevens en toestemming van de Autoriteit Persoonsgegevens bij doorgifte van persoonsgegevens naar landen buiten de EU.

### 2.9 ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing is er een crisisteam geïnstalleerd, in ieder geval bestaande uit de burgemeester en het Concern Management Team. De werkwijze dient te zijn vastgelegd.
- De gemeente Roermond participeert in allerlei landelijke platforms en onderhoudt o.a. contacten met de Informatiebeveiligingsdienst voor gemeenten (IBD) (nader toegelicht in hoofdstuk 3).

### 2.10 PDCA

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[9] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.
- De gemeente maakt gebruik van een ISMS bestaande uit een plan-do-check-act cyclus (PDCA-cyclus) om aantoonbaar grip te blijven houden op de diverse voorbereidende, uitvoerende, beherende en controlerende activiteiten die periodiek nodig zijn om informatieveiligheid naar een hoger niveau te tillen. Het inrichten en beheer van een ISMS ligt bij de CISO. Het ISMS ondersteunt de governance van de informatiebeveiliging.




*Figuur 2: Information Security Management System*

Toelichting figuur 2:

- **Plan**: De cyclus start met Informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de BIO en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het jaarplan en uitgewerkt in

7) Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
8) Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen
9) NEN/ISO 27001

het informatiebeveiligingsplan (Informatiebeveiligingsbeleid) van de gemeente. Afdelingsspecifieke activiteiten worden gepland in het afdelingsplan.

- **Do**: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- **Check** : Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.

  Externe controle: betreft controle buiten het primaire proces door een auditor.[10] Dit heeft het karakter van een steekproef. Jaarlijks worden diverse onderzoeken uitgevoerd, waarbij het Concern Management Team in principe opdrachtgever is. Bevindingen worden gerapporteerd aan het Concern Management Team.
- **Act**: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan Het Concern Management Team. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

## 3. Baseline Informatiebeveiliging Overheid

### 3.1 Algemeen

Het informatiebeveiligingsbeleid van de gemeente Roermond is gebaseerd op de 'Baseline Informatiebeveiliging Overheid', hierna te noemen BIO. Documentatie hierover is beschikbaar via de Informatiebeveiligingsdienst voor gemeenten (IBD)[11]. De gemeente heeft zich aangesloten op de dienstverlening van de IBD en bij de uitwerking van dit beleid zal zoveel mogelijk gebruik gemaakt worden van reeds beschikbare documentatie/handreikingen van de IBD. De IBD is de sectorale CERT / CSIRT[12] voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging.

Er zijn een aantal verschillen tussen BIO en de oudere BIG. Zo is de BIO gebaseerd op de ISO27002:2017, wat o.a. een andere nummering van de controls oplevert. Verder geeft de BIO meer vrijheid voor het treffen van passende maatregelen op basis van risicoanalyse. Zo kent de BIO, in tegenstelling tot de oude BIG, drie verschillende basisbeveiligingsniveau 's (BBN): BBN1, BBN2 en BBN3. Van ieder informatiesysteem dient bepaald te worden aan welk beveiligingsniveau voldaan dient te worden op basis van een risicoanalyse; de zogenaamde 'BBN-toets'. Het is de verantwoordelijkheid van elke proceseigenaar om ervoor te zorgen dat risico's binnen zijn proces passend worden beheerst op basis van de BIO.

Ieder beveiligingsniveau kent een aantal zogenaamde 'controls[13]', waarbij voor een hoger beveiligingsniveau tevens de controls voor alle daar onder liggende niveaus dienen te worden meegenomen. Aan iedere control zijn implementatiemaatregelen gekoppeld om deze uit te voeren.

Een ander belangrijk verschil met de BIG is dat er in de BIO meer verantwoordelijkheid wordt gelegd bij het lijnmanagement (clustermanagement). Deze is eindverantwoordelijk voor het uitvoeren van de noodzakelijke risicoanalyses (de BBN-toets) om het toepasselijke beveiligingsniveau vast te stellen en de bij dat risico behorende maatregelen.

### 3.2 Invulling door gemeente Roermond

Voor de gemeente Roermond betekent de invoering van de BIO als opvolger van de BIG de komende jaren het doorlopen van een leercurve. Zo dienen er een aantal inhaalslagen te worden uitgevoerd om documenten en procedures aan te passen op de nieuwe norm, zoals het indelen van alle informatiesystemen naar de nieuwe basisbeveiligingsniveau 's. Daartoe zullen de reeds uitgevoerde BIG 'baselinetoetsen' dienen te worden herzien naar de BBN-toets.

Wellicht de belangrijkste verandering zal zijn dat meer verantwoordelijkheid zal worden gelegd bij het lijnmanagement om te voldoen aan de BIO. Het Concern Management Team zal een belangrijke rol spelen bij de handhaving en controle van deze verantwoordelijkheid. De CISO en ISO zullen een meer coördinerende en adviserende rol krijgen dan voorheen het geval was.

## 4. Het risicomanagementproces binnen gemeente Roermond

### 4.1 Risicomanagement in de managementcyclus

Het proces informatiebeveiliging binnen de Gemeente Roermond is een cyclisch en iteratief proces (nader omschreven in paragraaf 2.13) dat start met het opstellen van een informatiebeveiligingsbeleid.

10) Van onder meer de IT auditor, de accountant (jaarrekening), rijksoverheid (voor bijv. basisregistraties) en interne auditors.
11) Zie www.ibdgemeenten.nl/downloads/
12) CERT = Computer Emergency Response Team; CSIRT = Computer Security Incident Response Team
13) De controls zijn een exacte kopie van die uit de ISO27002:2017

Aan de hand van de uitkomsten van Baselinetoets BBN BIO[14] op bestaande maatregelen en risicoanalyses wordt een Informatiebeveiligingsplan opgesteld en geactualiseerd. De in het Informatiebeveiligingsplan vastgestelde maatregelen zullen vervolgens geïmplementeerd moeten worden. Als laatste dienen deze maatregelen en hun implementatie te worden geëvalueerd. De evaluatie kan leiden tot bijstellingen in het Informatiebeveiligingsplan indien hiertoe aanleiding is op basis van de gevonden resultaten.

Risicomanagement binnen de informatiebeveiliging sluit aan bij de vastgestelde Nota Risicomanagement en Weerstandsvermogen. Bij beide is het doelbewuster te leren omgaan met risico's, deze meer systematisch in beeld te brengen en waar mogelijk beter te beheersen.

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in de besluitvorming. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht. Omdat risicomanagement is gebaseerd op historische en actuele informatie en op toekomstige verachtingen moet er uitdrukkelijk rekening gehouden worden met eventuele beperkingen en onzekerheden die aan deze informatie en verwachtingen verbonden zijn. Daarom dient ervoor gezorgd te worden dat informatie toegankelijk, juist, volledig, actueel, tijdig en toegankelijk moet zijn voor relevante belanghebbenden.

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden. Risico's kan men ontwijken, verkleinen, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie er ook gekozen wordt, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen dienen derhalve een kosten-batenanalyse te worden gemaakt.

Een doel van risicomanagement is het leren van ervaringen en op basis hiervan verbeteringen doorvoeren. Door te zoeken naar verbeterpunten en de wil om te leren kan de organisatie bouwen aan het doorlopend verhogen van de digitale weerbaarheid. Om verbeterpunten inzichtelijk te maken is het belangrijk dat resultaten gecontroleerd en geëvalueerd worden evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen. Controle is belangrijk om goed zicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed is in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp.

### 4.1.1 Risicoanalyse

Voor elk kritisch bedrijfsproces en informatiesysteem wordt door het lijnmanagement periodiek een risicoanalyse uitgevoerd. Het begrip lijnmanagement wordt hierbij ruim opgevat (zie paragraaf 2.3). De resultaten van een dergelijke risicoanalyse worden vastgelegd in een systeemontwerp c.q. informatiebeveiligingsplan.
Het uitgangspunt tijdens deze risicoanalyses is, dat middels een BBN-toets bepaald wordt welke betrouwbaarheidseisen (BIV: Beschikbaarheid – Integriteit – Vertrouwelijkheid) ) van toepassing zijn op het desbetreffende proces en informatiesysteem en binnen welk beveiligingsniveau deze vallen. Indien de eisen niet binnen het desbetreffende niveau vallen, maar hoger liggen dan geeft een diepgaande risicoanalyse uitsluitsel over welke additionele matregelen getroffen dienen te worden. Daarbij is het belangrijk vast te stellen, dat de situatie binnen de gemeente Roermond zélf het uitgangspunt is voor de analyses.

### 4.2 Toetsing en evaluatie

Informatiesystemen dienen regelmatig te worden gecontroleerd (ge-audit) op naleving van beveiligingsnormen. Audits en andere activiteiten waarbij controles dienen te worden uitgevoerd op operationele systemen dienen zorgvuldig te worden gepland en goedgekeurd om het risico van verstoringen van bedrijfsprocessen tot een minimum te beperken.
Gemeenten zijn verantwoordelijk voor de kwaliteit van hun informatiebeveiliging. Informatieveiligheid en privacybescherming hebben daarom een belangrijke plaats op de gemeentelijke agenda. Het adequaat inrichten van een verantwoordingsproces is daarbij essentieel. Gemeenten verantwoorden zich elk jaar

14) Om te bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis Beveiligings Niveau (BBN) heeft binnen de BIO, of meer maatregelen nodig heeft, nadat de GAP-analyse en impactanalyse ten opzichte van de BIO [ organisatie ] breed is uitgevoerd. Deze baselinetoets BIO bevat ook vragen om vast te kunnen stellen of er persoonsgegevens worden verwerkt en zo ja of er dan ook een DPIA nodig is.

over de kwaliteit van de informatieveiligheid van diverse informatiesystemen. In 2017 is hier voor het eerst de verantwoordingssystematiek ENSIA ingezet.

Uitgangspunt bij ENSIA is het horizontale verantwoordingsproces vanuit het college van burgemeester en wethouders aan de gemeenteraad. Deze horizontale verantwoording vormt dan de basis voor het verticale verantwoordingsproces aan de landelijke toezichthouders die een rol hebben in het toezicht op informatieveiligheid. Dit zijn het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Ministerie van Sociale Zaken en Werkgelegenheid (SZW), Ministerie van Infrastructuur en Waterstaat (I&W) en de Autoriteit Persoonsgegevens (AP).

De gemeente dient met ENSIA in één keer verantwoording af te leggen over de informatieveiligheid rondom het uitvoeren van de navolgende registratiesystemen (status juli 2022):

- Basisregistratie Personen (BRP);
- Reisdocumenten (voorheen PNIK);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Grootschalige Topografie (BGT);
- Basisregistratie Ondergrond (BRO);
- Waardering Onroerende Zaken (WOZ);
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet);
- Digitale persoonsidentificatie (DigiD).

### 4.2.1 Jaarlijks DigiD assessment

Betrouwbare digitale communicatie is van groot belang voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening. Het ministerie van BZK is verantwoordelijk voor de veiligheid van DigiD (Digitale Identiteit). Dit betreft niet alleen het middel zelf, maar ook de daarop aangesloten digitale diensten.
Met DigiD kan een natuurlijk persoon laten zien wie deze is als erop internet iets geregeld moet worden. Dat kan bij de overheid, het onderwijs, de zorg of een pensioenfonds.

Er wordt toezicht gehouden op de koppeling van DigiD met de webapplicatie van een aangesloten organisatie. Alle organisaties die DigiD gebruiken moeten per 1 augustus 2022 voldoen aan het DigiD Normenkader 3.0. Deze beveiligingsnorm is bedoeld voor organisaties die DigiD gebruiken en jaarlijks een ICT-beveiligingsassessment moeten doen. De norm is een selectie van richtlijnen uit het document 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het Nationaal Cyber Security Centrum (NCSC). De norm is vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, AuditDienstRijk en het NCSC. Toetsing van de normen gebeurt op basis van een IT-audit uit te voeren door een onafhankelijk bij de beroepsgroep NOREA aangesloten IT-auditor.

Een organisatie met een DigiD aansluiting:
- laat jaarlijks een assessment uitvoeren; Voor bestaande DigiD aansluitingen maakt dit assessment deel uit van ENSIA;
- zorgt voor het oplossen van eventuele tekortkomingen;
- levert een door een RE-auditor opgestelde en ondertekende rapportage aan bij Logius.

Met het ICT-beveiligingsassessments DigiD houdt Logius toezicht op de DigiD aansluitingen met als doel het gebruik van DigiD veilig te houden. Logius houdt ook toezicht op het op tijd naleven van de assessmentplicht en beoordeelt de IT-auditrapportage (assessmentrapportage).

Het ICT-beveiligingsassessments DigiD biedt inwoners meer zekerheid dat DigiD als authenticatiemiddel veilig en betrouwbaar is. Het verplicht DigiD aansluithouders inzicht te geven in de informatieveiligheid van de op DigiD aangesloten webapplicatie.

### 4.2.2 Onafhankelijke beoordeling van Informatiebeveiliging

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld.

De werkzaamheden voor de interne audits zijn opgenomen in het ‘Jaarplan Audit en Interne Controle’ Gemeente Roermond. Interne audits is de verzamelnaam voor alle beheersmatige activiteiten die nodig

zijn om processen en activiteiten binnen een organisatie te beheersen, te sturen en te verbeteren. Interne controle is daarom aanwezig op alle niveaus, van medewerker tot en met Gemeentesecretaris. De verplichte audits dienen in de afdelingsplannen te worden opgenomen wat ertoe leidt dat er periodiek over gerapporteerd moet worden. Door de Plan-Do-Check-Act cyclus van (interne) audits wordt gezorgd voor het borgen van processen en een verdere doorontwikkeling van onder andere informatiebeveiliging.

De implementatie van de Informatiebeveiliging wordt onafhankelijk beoordeeld.
Deze activiteiten worden door geautoriseerde medewerkers binnen de gemeente uitgevoerd (interne controle afdeling, functioneel en technisch beheerders, Functionaris voor de Gegevensbescherming).
Het betreft:

- controle op de naleving van wettelijke en contractuele voorschriften;
- monitoren van de performance en de meldingen van de infrastructuur;
- controle op naleving van de beveiligingsrichtlijnen;
- controle op het hanteren van de juiste procedures;
- controle op het gebruik van de juiste ICT middelen.

Op de Informatiebeveiliging worden periodiek beveiligingsaudits uitgevoerd in opdracht van het lijnmanagement. Hiervoor worden afspraken gemaakt over de opdrachtverstrekking, de toetsingskaders en de uitvoering.
De (onafhankelijke) beoordeling c.q. toetsing moet uitsluitsel geven over:

- het Informatiebeveiligingsplan: elke beheerder van een bedrijfskritische applicatie moet beschikken over een plan dat voldoet aan de in het informatiebeveiligingsbeleid gestelde eisen.
- alle vastgestelde maatregelen: of deze daadwerkelijk en op de juiste wijze zijn geïmplementeerd.
- alle getroffen maatregelen: in welke mate deze afdoende en toereikend zijn. Daarbij moet speciaal aandacht geschonken worden aan de toegang van derden tot de infrastructuur en gegevens en de uitbesteding van ICT-diensten.
- de uitgevoerde risicoanalyses. Die moeten voor alle verantwoordelijkheidsgebieden c.q. informatiesystemen uitgevoerd zijn, waarbij de afhankelijkheden, de bedreigingen, de eisen en de te nemen maatregelen voor Informatiebeveiliging zijn vastgelegd en vastgesteld.

Randvoorwaarde
De audit van de beveiliging van ICT-voorzieningen dient zo min mogelijk inbreuk te plegen op de beschikbaarheid, de vertrouwelijkheid en de integriteit van de ICT-voorzieningen.

*Aldus vastgesteld door burgemeester en wethouders van de gemeente Roermond op 28 november 2023.*

*Het college van burgemeester en wethouders,*

*de secretaris,*
*J. van Putten*

*de burgemeester,*
*Y.F.W. Hoogtanders*