Gemeente
De Ronde Venen

# (Strategisch) Beleid informatieveiligheid Gemeente De Ronde Venen 2022-2026

| | |
|---|---|
| Versie | 1.0 |
| Auteur: | Patrick Zuiderwijk (CISO) – team Concerncontrol |
| Vastgesteld: | 6 december 2022<br>door het College van B&W van Gemeente De Ronde Venen. |

# Managementsamenvatting

De Ronde Venen heeft als gemeente een maatschappelijk belangrijke functie en is verplicht om de informatie in gemeentelijke processen goed te beschermen. De privacywet AVG (2018) stelt hoge eisen aan de bescherming van persoonsgegevens en geeft de landelijke toezichthouder de bevoegdheid tot het opleggen van zware boetes. Door de steeds verdergaande technologische ontwikkelingen worden bedrijfsprocessen steeds afhankelijker van informatiesystemen. Informatiebeveiliging is daarmee een belangrijke randvoorwaarde voor het bereiken van de doelen die de gemeente zichzelf stelt. Daarom investeert de gemeente in informatiebeveiliging, om betrouwbare, transparante en veilige diensten te kunnen verlenen aan inwoners en bedrijven. Omdat niet alles tegelijk kan worden aangepakt, moet de gemeente prioriteiten stellen. Daarvoor benoemt dit beleidsdocument de volgende vier speerpunten:

1. **Risicogebaseerd werken:** de gemeente organiseert informatiebeveiliging zodanig dat steeds de afweging gemaakt wordt tussen *enerzijds* de relevante bedreigingen, met de kans op schade en *anderzijds* de kosten van mitigerende maatregelen om de restrisico's acceptabel te houden.
2. **Bewust verantwoordelijkheid nemen:** de organisatie handelt op basis van de lijnverantwoordelijkheid voor informatiebeveiliging, met duidelijk ingevuld eigenaarschap. Goede verantwoording betekent dat Informatieveiligheid is opgenomen in de integrale P&C-cyclus.
3. **Security by design:** de gemeente zorgt dat de risico's van informatiebeveiliging vanaf het begin bij innovatie en veranderingen meegenomen wordt, dus vanaf de ontwikkeling van beleid, het inrichten van processen tot en met het uitfaseren van informatiesystemen. Het gaat bijvoorbeeld om dataminimalisatie, het *need-to-know* principe en transparantie van ontwerp.
4. **Lerend vermogen:** in de snel veranderende wereld van cybersecurity moeten bedrijfsprocessen zijn opgewassen tegen de dreigingen van morgen. Dit stelt eisen aan de beveiliging in de gemeente De Ronde Venen, zoals beschikbare kennis en expertise, inrichting op basis van structurele risicoanalyses, de toetsing en hoe effectief de gemeente die beveiliging kan bijstellen.

Gelet op de bovenstaande speerpunten zijn goed opgeleide professionals met actuele kennis in informatiebeveiligingsfuncties cruciaal. Vandaar dat de gemeente zich specifiek zal richten op het opleiden van haar medewerkers.

Naast het opleiden van de medewerkers zijn gedrag, attitude en cultuur essentieel om de gewenste ambities te behalen. De komende jaren zal het onderwerp bewustwording of awareness dan ook prominent op de agenda staan. Hierbij werkt de gemeente aan een open organisatiecultuur waarin het vertrouwen er is om risico's en incidenten zo snel mogelijk te melden ('Je bent een held als je meldt') en kennis uit te wisselen. Zo kan worden voorkomen dat de beheersing van informatiebeveiliging uit de hand loopt. De *'Tone at the Top'* en het voorbeeldgedrag van het management is daarbij van wezenlijk belang.

Voor het inrichten van een adequate beveiliging is betrouwbare informatie nodig over de risico's en mogelijke kwetsbaarheden in de organisatie. Daarbij is een goede koppeling met privacy essentieel, om te voorkomen dat er verschillende beelden ontstaan over de veiligheid van de gemeente.

Het jaarlijkse privacy & informatieveiligheidsplan dat de directie vaststelt, werkt strategische, tactische en operationele onderdelen van informatiebeveiliging verder uit. Dit wordt gedaan op basis van onder andere input van het lijnmanagement in de gemeentelijke organisatie, het actuele dreigingsbeeld, de uitkomsten van audits en de beschikbare middelen. Daarin staan ook de geplande acties om de beveiliging in lijn te brengen met de ambitie in het beleid en de relevante wet- en regelgeving.

# Inhoudsopgave

# 1. Inleiding

Dit beleidskader beschrijft het strategisch informatieveiligheidsbeleid voor de jaren 2022 – 2026 en vervangt het vorige beleidsdocument voor informatieveiligheid (College van B&W, 11 december 2018).

Dit beleid is richtinggevend en kaderstellend en wordt uitgewerkt met specifieke interne beleidsdocumenten voor informatieveiligheid op strategisch en tactisch niveau en werkinstructies op operationeel niveau. Met dit '(Strategisch) Beleid informatieveiligheid Gemeente De Ronde Venen 2022-2026' zet de gemeente De Ronde Venen een volgende stap om de beveiliging van persoonsgegevens en andere gevoelige en vertrouwelijke informatie binnen de processen verder te verbeteren en te voldoen aan het wettelijk kader.

Als basis voor de inhoud van dit strategisch beleidskader zijn de NEN-ISO/IEC 27002 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) gebruikt. Met het hebben van een actueel en vastgesteld informatieveiligheidsbeleid wordt voldaan aan BIO-maatregel 5.1.

### 1.1 Bestuurlijke uitgangspunten

VEILIGHEID[1]
Veilig zijn en je veilig voelen zijn eerste levensbehoeften en noodzakelijk om jezelf te zijn en jezelf te ontwikkelen. Er is dan ook continu aandacht voor preventie om De Ronde Venen een veilige en fijne (woon) omgeving te maken. Veiligheid is een breed begrip. Dit gaat behalve over wetten, regels en de handhaving hiervan ook over zaken als overlast, overtredingen, criminaliteit en ondermijning.

HANDHAVING OPENBARE ORDE EN VEILIGHEID[2]
Wij geven prioriteit aan een digitaal weerbare gemeente. We zetten ons in om te voorkomen dat inwoners en bedrijven slachtoffer worden van cybercrime en gedigitaliseerde criminaliteit. Ook zorgen we ervoor dat de informatiebeveiliging van de gemeente op orde is en dat we goed voorbereid zijn op cybercrisis en online aangejaagde ordeverstoringen.

BEDRIJFSVOERING, DIENSTVERLENING EN ICT[3]
Een overheid moet betrouwbaar zijn.
(..) We gaan zorgvuldig met gegevens van inwoners om. We houden hun gegevens veilig. We investeren in de ICT om dit op een kwalitatief goede manier mogelijk te houden. De organisatie moet op dit gebied up-to-date en veilig zijn en blijven

Samen voor elkaar- ONZE VISIE[4]
Wij zijn een organisatie die integraal en resultaatgericht werkt aan de opgaven van de gemeente. We stellen de samenleving centraal. We zijn betrouwbaar, zowel voor ons bestuur als voor onze inwoners. We werken met professionele, krachtige, zelfstandige medewerkers die elkaar helpen om alle uitdagingen het hoofd te bieden.

[1] 'In het hart' Coalitieakkoord 2022-2026, pagina 19
[2] 'In het hart' Coalitieakkoord 2022-2026, pagina 21
[3] 'In het hart' Coalitieakkoord 2022-2026, pagina 25
[4] 'Samen voor elkaar', pagina 19

Dat doen we in een permanent proces van leren en ontwikkelen. Met aandacht voor verschillen in tempo en veranderende omstandigheden. We zijn een fijne werkorganisatie. We stimuleren durf en creativiteit en bieden comfort. We helpen onze professionals steeds autonomer te werken, in verbinding met elkaar en de omgeving. We zijn flexibel en leveren maatwerk waar dat kan.

### 1.2 Wat is informatiebeveiliging?

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Informatiebeveiliging verhoogt de kwaliteit van onze data en dienstverlening door aspecten zoals efficiency, effectiviteit, controleerbaarheid, bruikbaarheid, onderhoudbaarheid en portabiliteit. Het beperkt zich zeker niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, inwoners, ondernemers, gasten, bezoekers en externe relaties.

### 1.3 Bestuurlijke ambitie informatiebeveiliging

De gemeente De Ronde Venen heeft nadrukkelijk aandacht voor de impact van digitalisering op haar processen, zodat bijvoorbeeld informatie met in- en externe (keten)partijen eenvoudig en veilig kan worden gedeeld. Enerzijds biedt dit kansen om de processen effectiever en efficiënter te maken. Anderzijds maakt digitalisering de processen meer afhankelijk van ICT-middelen en dat stelt hogere eisen aan de informatiebeveiliging en privacybescherming. Bovendien omvat informatiebeveiliging meer dan alleen ICT-systemen en is het vakgebied van momenteel sterk in beweging door steeds verdergaande ontwikkelingen, zoals veranderende wet- en regelgeving, plaats en tijd onafhankelijk werken en datagericht sturen. Daarom streeft de gemeente naar continue verbetering van de beveiliging van haar processen.

Omdat niet alles tegelijk kan worden aangepakt, stelt de gemeente prioriteiten op basis van de context, de gestelde eisen aan de processen en de voorzienbare ontwikkelingen. Daarvoor benoemt dit beleidsdocument de volgende vier speerpunten:

1. **Risicogebaseerd werken:** de gemeente organiseert informatiebeveiliging zodanig dat steeds de afweging gemaakt wordt tussen enerzijds de relevante bedreigingen met de kans op schade en anderzijds de kosten van mitigerende maatregelen om deze restrisico's acceptabel te houden.
2. **Bewust verantwoordelijkheid nemen:** de organisatie handelt op basis van de lijnverantwoordelijkheid voor informatiebeveiliging, met duidelijk ingevuld eigenaarschap. Goede verantwoording betekent dat Informatieveiligheid is opgenomen in de integrale P&C-cyclus.
3. **Security by design:** de gemeente zorgt dat de risico's van informatiebeveiliging vanaf het begin bij veranderingen meegenomen wordt, dus vanaf de ontwikkeling van beleid, het inrichten van processen tot en met het uitfaseren van informatiesystemen. Het gaat bijvoorbeeld om dataminimalisatie, het *need to know* principe en transparantie van ontwerp.
4. **Lerend vermogen:** in de snel veranderende wereld van cybersecurity moeten bedrijfsprocessen zijn opgewassen tegen de dreigingen van morgen. Dit stelt eisen aan de beveiliging in de gemeente De Ronde Venen, zoals beschikbare kennis en expertise, inrichting op basis van structurele risicoanalyses, de toetsing en hoe effectief de gemeente die beveiliging kan bijstellen.

### 1.4 Doel van het beleid, doelgroep en leeswijzer

Het doel van dit beleid is de professionele samenwerking rondom informatiebeveiliging te sturen zodat de gemeente De Ronde Venen een veilige informatievoorziening kan inrichten die voldoet aan de gestelde eisen voor beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Daarmee kan de gemeente veilige diensten leveren aan bedrijven, organisaties, (keten)partners en inwoners en is continuïteit van de uitvoering van haar wettelijke taken geborgd. Het strategische beleid is bedoeld als kader voor het inrichten en managen van de informatiebeveiliging op tactisch en operationeel niveau.

De doelgroepen voor het strategisch beleid zijn ook degenen die een primair belang hebben met informatiebeveiliging: de gemeenteraad, het College van B&W, de directie, teammanagers en de medewerkers van de Gemeente De Ronde Venen.

Hoofdstuk 2 beschrijft de context van het beleid, waarna hoofdstuk 3 het strategisch beleid uitwerkt. Hoofdstuk 4 beschrijft de taken en verantwoordelijkheden voor informatiebeveiliging en privacybescherming binnen de gemeentelijke organisatie. Bijlage 1 bevat bevat de definities van gebruikte termen en afkortingen in dit document en bijlage 2 geeft de huidige functiematrix informatieveiligheid aan.

### 1.5 Reikwijdte van dit beleid

Het Informatieveiligheidsbeleid geldt voor gemeentelijke informatie tijdens de hele levenscyclus in alle processen van de gemeente, ongeacht de toegepaste technologie voor opslag (ICT systemen inclusief papieren dossiers en menselijke kennis) en of deze informatie intern of extern (via outsourcing of ketenpartners) wordt verwerkt. Het dekt dus ook aanvullende beveiligings-eisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK), DigiD (Digitale Identiteit) en Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI, DigiD en gemeentelijke basisregistraties). Deze eisen worden in aanvullende documenten geformuleerd.

Voor gegevensbescherming (privacy) en het naleven van de Algemene Verordening Gegevensbescherming (AVG) is separaat beleid opgesteld (Privacybeleid De Ronde Venen 2022, College van B&W, 13 september 2022). Daar waar gegevensbescherming en informatiebeveiliging elkaar overlappen, moet de documentatie en procesinrichting aantoonbaar voldoen aan de eisen van zowel het privacy- als het Informatieveiligheidsbeleid.

### 1.6 Actualisering van het beleid

Dit beleidsdocument is door het College van B&W vastgesteld voor de periode van 2022-2026 en dient door alle organisatieonderdelen en bestuur en alle medewerkers te worden nageleefd.
Als eigenaar van dit beleidsdocument roept de CISO iedereen binnen de doelgroep op om suggesties en verbeteringen in te sturen. Uiterlijk het laatste jaar van de geldigheid wordt dit beleid geëvalueerd, waar nodig aangepast en opnieuw vastgesteld. Interne informatie uit audits, penetratietesten (hierna: pentest) en andere privacy- en securityevaluaties leveren eveneens input voor de bijstelling van dit document. Ontwikkelingen in de maatschappij en security research vormen externe input voor de beleidsevaluatie.

# 2. Context van het beleid voor informatiebeveiliging

Een beleidsdocument voor informatiebeveiliging staat niet op zichzelf; de inhoud ervan is afhankelijk van wet- en regelgeving en standaarden voor informatiebeveiliging. Daarnaast is de formulering van het beleid afhankelijk van 'wat werkt' in de organisatie en hoe de context zich ontwikkelt. De inhoud van de volgende documenten is van belang voor de actualisering van het Informatieveiligheidsbeleid van de Gemeente De Ronde Venen.

### 2.1 Gerelateerd beleid bij de Gemeente De Ronde Venen

- Visie op informatievoorziening (2018-2022), vastgesteld in College van B&W, november 2018;
- Privacybeleid De Ronde Venen 2022, vastgesteld in College van B&W, 13 september 2022;
- Addendum privacybeleid De Ronde Venen 2022, vastgesteld in College van B&W, 13 september 2022;
- Visie op control en de financiele functie, vastgesteld in directie, 26 oktober 2022;
- Raamwerk informatiebeheer, vastgesteld in directie, 3 augustus 2022;
- Beleid en procedures veilig gebruik Suwinet-inkijk 2019-2022, vastgesteld in College van B&W, 4 februari 2020

### 2.2 Standaarden voor informatiebeveiliging

De basis voor de inrichting van het Informatieveiligheidsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van 'best practices' bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun Informatieveiligheidsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Omdat de huidige ISO 2700x-normenset in 2013 is opgesteld, wordt verwacht dat de International Standards Organisation binnenkort deze normen zal actualiseren (NEN-ISO/IEC 27002:2022). Dit zal (op termijn) gevolgen hebben voor de bestaande operationele inrichting van informatiebeveiliging die is gebaseerd op de huidige versie van de BIO.

### 2.3 Baseline Informatiebeveiliging Overheid (BIO)

De BIO is het normenkader informatiebeveiliging voor de gehele overheid en is gericht op risicomanagement. De BIO bestaat uit een baseline met drie niveaus van beveiliging. Vergelijkbaar met de AVG is de meerwaarde van de BIO dat dezelfde norm bij alle overheidsorganisaties verplicht is, waardoor het veilig delen van informatie veel eenvoudiger wordt.

### 2.4 Dreigingsbeeld informatiebeveiliging en cybersecurity

Het Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2023/2024[5] geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Daarnaast geeft de NCTV jaarlijks het Cybersecuritybeeld Nederland (CSBN)[6] uit.

Deze dreigingsbeelden worden periodiek geactualiseerd en helpen de Gemeente De Ronde Venen om strategisch en tactisch beleid en plannen voor informatiebeveiliging te actualiseren en focus te leggen bij de uitvoering ervan.

### 2.5 Wetgeving en regelgeving voor informatiebeveiliging

De volgende wetgeving heeft raakvlakken met de informatiebeveiliging binnen de gemeentelijke context.Hier moet de gemeente dus ook aan voldoen:

De **Algemene Verordening Gegevensbescherming (AVG)** is op 25 mei 2018 in werking getreden. Volgens de AVG moeten organisaties passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen en zo datalekken te voorkomen. De Autoriteit Persoonsgegevens (AP)kan organisaties die de beveiliging niet op orde hebben en daarmee de AVG overtreden een boete opleggen.

**De Wet Computercriminaliteit II en III** zijn in 2006 resp. 2018 van kracht geworden. De wetten voorzien in wijzigingen in het Wetboek van Strafrecht en Strafvorderingen om een betere aanpak van computercriminaliteit mogelijk te maken.

**Archiefwet** (1995) regelt dat archiefbescheiden lange tijd beschikbaar en raadpleegbaar blijven. Het archiefbesluit noemt een termijn van tenminste 100 jaar[7]. Deze termijn geldt overigens slechts voor *door de overheid opgemaakte, permanent* te bewaren archiefbescheiden en geldt daarom niet voor de *ontvangen* archiefbescheiden. Voor de duurzaamheid van de op termijn te vernietigen archiefbescheiden en ontvangen archiefbescheiden gelden geen bijzondere eisen. Wel moeten ook deze bescheiden in goede, ordelijke en toegankelijke staat worden gehouden (art. 3 Archiefwet).

**Wet Elektronisch Bestuurlijk Verkeer** (2004) is een aanvulling op de Algemene Wet Bestuursrecht en bevat regels over het verkeer langs elektronische weg tussen inwoners en bestuursorganen en tussen bestuursorganen onderling. De wet formuleert abstracte (techniekonafhankelijke) normen waaraan het elektronische verkeer moet voldoen teneinde voldoende beveiligd te zijn. Voldoende beveiligd wil zeggen: minstens even betrouwbaar als schriftelijk verkeer. Berichten die langs elektronische weg door bestuursorganen worden verzonden, dienen in voldoende mate beveiligd te zijn. Eveneens dienen berichten die aan een bestuursorgaan worden gestuurd, door dat bestuursorgaan van de hand te kunnen worden gewezen indien het bestuursorgaan vermoedt dat het bericht in onvoldoende mate is beveiligd. Naar verwachting zal de geactualiseerde wet op 1 januari 2023 in werking treden.

---

[5] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

[6] https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

[7] De Rijksoverheid werkt aan nieuwe Archiefwet (invoering verwacht begin 2024). Daarin komt onder meer te staan dat overheidsinformatie die we blijvend willen bewaren, al na 10 jaar worden overgebracht naar de openbare archieven.

**Wet op de politiegegevens** (2007) regelt de verwerking van persoonsgegevens voor opsporingsdoelen door buitengewoon opsporingsambtenaren (BOA's). De Wpg gebiedt de noodzakelijkheid, rechtmatigheid en doelbinding bij de verwerking van deze gegevens en vraagt daarbij om de juistheid, volledigheid en beveiliging van deze verwerkingen.

**Digitale Identiteit (DigiD)** (2016) is het standaardidentificatie- en authenticatiemechanisme bij gegevensuitwisseling met de overheid via internet. Daarmee bestaat DigiD uit een enorme directory van digitale identiteiten. Bovendien staat de overheid borg voor de betrouwbaarheid van die identiteiten. Voor de beveiliging van de DigiD-aansluitingen heeft Logius (BZK) een normenkader opgesteld waar de gemeente aan moet voldoen. Hierin veel aandacht voor webapplicatie gerelateerde onderwerpen zoals data-eigenaarschap, dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.

Beveiligingseisen in **overige wet- en regelgeving** die voor bepaalde processen relevant is:

- Paspoorten en Nederlandse identiteitskaarten (PNIK);
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI);
- Basisregistraties: personen (BRP), Adressen en Gebouwen (BAG), Grootschalige Topografie (BGT), Ondergrond (BRO), Wet waardering onroerende zaken (WOZ);
- GIBIT - Informatiebeveiliging in leveranciersrelaties (BIO hoofdstuk 15);
- Programma van Eisen PKI Overheid;
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie;
- Wet bescherming klokkenluiders.

### 2.6 Industriestandaards voor informatiebeveiliging

De **Informatiebeveiligingsdienst** (IBD) van de VNG publiceert handreikingen en aanvullingen op de BIO.

Het **Centrum Informatiebeveiliging en Privacybescherming** (CIP) publiceert onder andere uitwerkingen van BIO-maatregelen. Deze dienen als handreiking.

Het **Nederlandse Beroepsorganisatie van Accountants (NBA) volwassenheidsmodel informatiebeveiliging** geeft informatie, sturing en beheersing van informatiebeveiliging en wordt al jaren binnen de Nederlandse overheid gebruikt. Het model is gebaseerd op de volgende vragen:

1. Op welk volwassenheidsniveau zou uw organisatie gelet op de risico's zich moeten bevinden?
2. Op welk volwassenheidsniveau bevindt uw organisatie zich momenteel?
3. Wat heb ik nodig om een hoger volwassenheidsniveau te bereiken?

Met dit NBA-model kan een organisatie vraag 2 en 3 beantwoorden. Binnen hun eigen context moeten organisaties zelf met een risicoanalyse het volwassenheidsniveau bepalen, met het daarvoor benodigde budget. Het niveau van volwassenheid is een maat voor de beheersing van informatiebeveiliging, dus de mate waarin de organisatie 'in control' is en kan blijven. De uitwerking van het actuele en gewenste volwassenheidsniveau zal in het jaarrapport privacy en informatieveiligheid geschieden.
Het volwassenheidsmodel is niet bedoeld als een nieuw normenkader: het gebruikt of verwijst naar bestaande *'good practices'*, zoals COBIT, NEN-ISO/IEC 27001 en BIO. De NBA evalueert het model periodiek en stelt waar nodig bij.

Het **Nationale Cyber Security Centrum** (NCSC) publiceert veel over cybersecurity, zoals de Handreiking Cybersecuritymaatregelen.

# 3. Strategisch beleid informatiebeveiliging

### 3.1 Basisprincipes voor informatiebeveiliging

Gemeente De Ronde Venen hanteert de volgende basisprincipes voor haar informatiebeveiliging. Deze zijn van toepassing op de gehele gemeentelijke organisatie en op alle partijen waarmee de gemeente samenwerkt, inclusief ketenpartners en leveranciers en fungeren als basis om de ambities van de gemeente De Ronde Venen te realiseren.

1. *Eigenaarschap en lijnverantwoordelijkheid:*
   alle processen, ICT-applicaties, webapplicaties (zoals DigiD), informatieverzamelingen en de generieke infrastructuur (fysiek en virtueel) hebben elk één formele eigenaar in de lijnorganisatie. Informatiebeveiliging is binnen elk onderdeel van de organisatie een lijnverantwoordelijkheid. Het management bevordert een veilige cultuur en laat maatregelen nemen zodat de processen voldoen aan vastgestelde beveiligingseisen.
2. *Informatiebeveiliging is een continu proces:*
   informatiebeveiliging ondersteunt de organisatie in het bereiken van haar doelstellingen. De 'Plan-Do-Check-Act'-cyclus is de basis van het managementsysteem om informatie-beveiliging te verbeteren (ISMS). Door periodieke controle, organisatiebrede planning én coördinatie van de uitvoering wordt de veiligheid van de informatievoorziening geborgd binnen de organisatie.
3. *Voldoende middelen:*
   informatiebeveiliging kost geld en capaciteit. Regels en verantwoordelijkheden voor het inrichten en gebruiken van de beveiliging dienen te worden vastgesteld. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen conform dit beleid te kunnen beveiligen.
4. *Complete levenscyclus:*
   Informatiebeveiliging is een vast en onlosmakelijk onderdeel van vernieuwing en beheer van processen.
5. *Basisbeveiligingsniveau:*
   net als veel overheidsorganisaties heeft de Gemeente De Ronde Venen een **lage risicobereidheid**, wat betekent dat de gemeente alleen bereid is lage risico's te nemen om haar doelstellingen te realiseren. De gemeente De Ronde Venen beschikt daarom over een relatief hoog basisbeveiligingsniveau (**BIO-BBN2**), dat geldt voor alle vormen van informatieverwerking. Als dit niveau voor bepaalde informatie niet nodig is, moet die informatie expliciet als zodanig worden gelabeld.
6. *Doelmatigheid:*
   maatregelen voor informatiebeveiliging kosten geld en capaciteit van de organisatie. Er moeten doelmatige, zakelijke argumenten zijn om beveiligingsmaatregelen te treffen zodat de kosten in balans zijn met het te beschermen belang. Dit betekent dat een risicoanalyse de noodzaak van passende maatregelen moet aantonen.
7. *Verantwoordelijkheid medewerkers:*
   informatiebeveiliging is van iedereen. Alle medewerkers, zowel vast als tijdelijk, intern of extern, zijn verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, verandering of verlies. Bovendien moet elke medewerker incidenten en risico's voor informatiebeveiliging melden (*Je bent een held als je meldt*). Voor handelingen in zakelijke ICT-systemen is iedere medewerker identificeerbaar, zodat monitoring en controles op het juiste gebruik kunnen worden ingericht, zonder dat de persoonlijke levenssfeer wordt aangetast. De medewerkers zijn hiervan op de hoogte.

8. *Risicobewustzijn:*
   aandacht voor bewustwording en opleiding is een onmisbaar onderdeel van de inrichting van informatiebeveiliging. Managers zijn verantwoordelijk voor de ontwikkeling van expertise binnen hun teams, zodat zij hun verantwoordelijkheid effectief kunnen invullen.
9. *Samenwerking met privacybescherming:*
   ontoereikende beveiliging van persoonsgegevens kan leiden tot datalekken, die overlast veroorzaken voor betrokkenen en het vertrouwen van burgers in de overheid schaden. Daarnaast kunnen incidenten schade veroorzaken en kan de Autoriteit Persoonsgegevens hoge boetes opleggen wanneer de beveiliging tekortschiet.

### 3.2 Risicogebaseerde informatiebeveiliging

Risico wordt bepaald op basis van kans op een incident en de impact daarvan. Om de impact van het risico te bepalen bevat de 'Baselinetoets BBN BIO' de criteria voor de BIV-aspecten. Informatiebeveiliging dient risicogebaseerd te worden opgezet en ingericht, conform het speerpunt van dit beleidskader. De risico's van bedreigingen waartegen informatie moet worden beschermd worden afgeleid uit de antwoorden op de volgende vragen:

1. Wat zijn voor ons de meest waardevolle processen, informatiesystemen en informatie?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze meest waardevolle informatiesystemen en informatie?
3. Wat doen we wel en vooral ook niet om deze informatiesystemen en informatie te beschermen tegen deze gebeurtenissen?

De gemeente neemt maatregelen om bijvoorbeeld te voorkomen dat informatie onterecht wordt gewijzigd of dat de informatieverwerking wordt verstoord. Om te zorgen dat deze maatregelen effectief en efficiënt zijn, neemt de gemeente De Ronde Venen maatregelen op basis van het risico (met een kosten-batenoverweging) óf omdat wet- en regelgeving daartoe verplicht. Dat betekent dus ook dat de gemeente de incidenten met informatiebeveiliging moet registeren in een zogenaamd *incidentregister*.

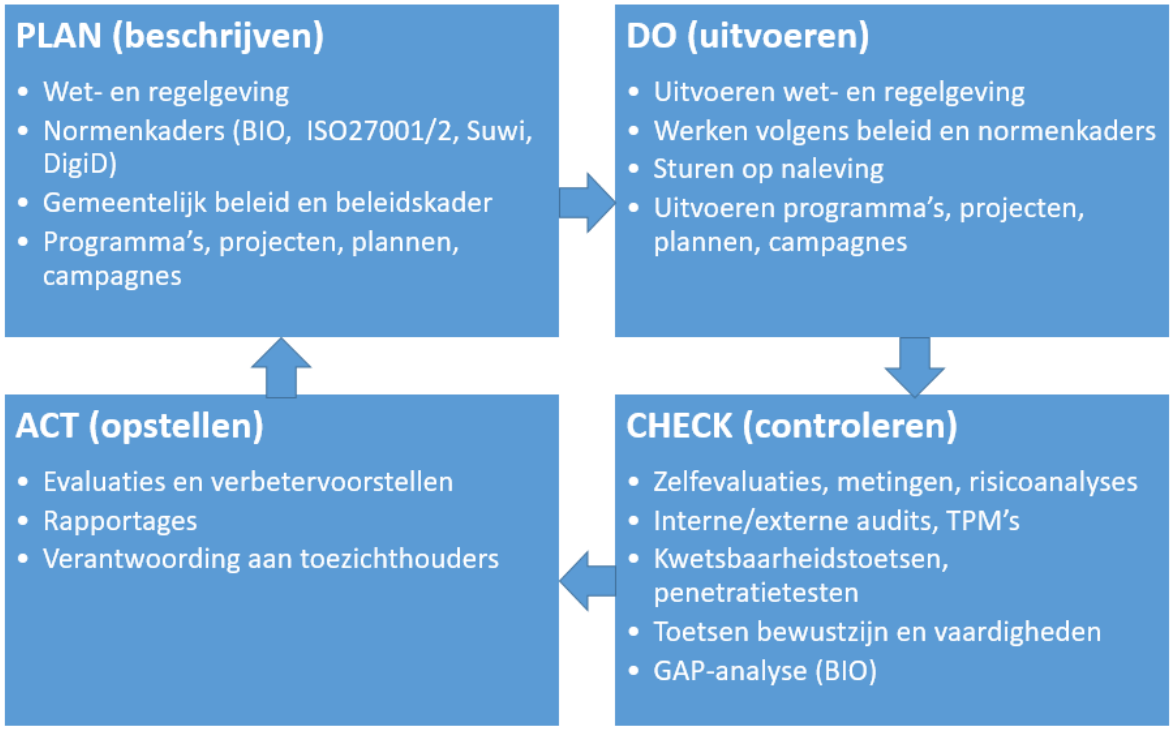
Ook al zoekt Gemeente De Ronde Venen - bijvoorbeeld met pentesten - preventief naar kwetsbaarheden, daarmee zijn niet alle incidenten te elimineren. Daarom heeft Gemeente De Ronde Venen een procedure nodig voor afhandeling van incidenten (inclusief de opschaling naar een ICT-crisis) en oefent periodiek met een cyberaanval. Omdat risicomanagement inherent een bepaalde mate van onzekerheid kent, moet het management continu afwegen of de ingerichte beveiliging van processen voldoet aan de eisen die de organisatie stelt voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De Chief Information Security Officer (CISO) en team I&A ondersteunen het management bij het plannen, inrichten, controleren en evalueren van de informatiebeveiliging. Gemeente De Ronde Venen heeft een CISO aangesteld conform het VNG CISO-functieprofiel.

### 3.3 Hoe beveiligt de Gemeente De Ronde Venen haar informatie?

Een goede beveiliging van informatie stelt eisen aan het beveiligingsproces. De volgende paragrafen beschrijven de te nemen processtappen met daaraan verbonden acties, die de 'Plan-Do-Check-Act'-cyclus sluitend moeten maken.

- Plan: omschrijf het gewenste resultaat;
- Do: duidelijk is welke acties nodig zijn om het gewenste resultaat te bereiken;
- Check: de gevolgen van de genomen acties zijn duidelijk vast te stellen;
- Act: de eventueel noodzakelijke aanpassingen kunnen helder worden afgeleid.

De toegepaste PDCA-cyclus voor informatiebeveiliging is hieronder samenvat.




**Inventariseren en classificeren van bedrijfsprocessen en ondersteunende systemen**

Om de beveiliging op basis van risicomanagement in te richten moet Gemeente De Ronde Venen in beeld hebben welke processen, applicaties en systemen de organisatie gebruikt en welke beveiligingseisen (BIV) de organisatie aan deze processen stelt. Vanuit het uitgangspunt van risicomanagement krijgen processen, applicaties en systemen die als bedrijfskritisch (kroonjuwelen) zijn geclassificeerd prioriteit bij het inrichten van de beveiliging en het herstel bij incidenten.

**Analyse van beveiligingsrisico's**

De eigenaar van het bedrijfsproces of informatiesysteem moet een analyse van de risico's uitvoeren. Ligt de nadruk op privacy, dan wordt dit een Privacy Impact Assessment (DPIA - Data Protection Impact Assessment) genoemd, die onder andere ook de rechtmatigheid van de verwerking toetst. De CISO kan ondersteuning leveren voor het uitvoeren van de risicoanalyse, die specificeert welke beveiligingsmaatregelen de eigenaar moet treffen voor een adequate beveiliging.

Een risicoanalyse moet in principe iedere drie jaar worden geactualiseerd of eerder, bijvoorbeeld als het betreffende proces sterk verandert, nieuwe informatiesystemen in gebruik worden genomen of een opgetreden beveiligingsincident aantoont dat de beveiliging moet verbeteren.

**Het inrichten van beveiligingsmaatregelen**
Beveiligingsmaatregelen kunnen worden geselecteerd, bijvoorbeeld uit de BIO. De eigenaar wijst een of meer medewerkers aan die belast worden met het inrichten van de beveiligings-maatregelen en ziet erop toe dat de beveiliging tijdig op orde is.

**Evaluatie en controle**
Informatiebeveiliging is een dynamisch proces, waarbij het niet volstaat om eenmalig de gekozen beveiligingsmaatregelen in te richten. Bijvoorbeeld: de AVG verplicht organisaties persoonsgegevens aantoonbaar goed te beveiligen. Bedrijfskritische systemen of systemen die bijzondere persoonsgegevens verwerken moeten daarom periodiek worden onderzocht op kwetsbaarheden en de effectiviteit van ingerichte beveiligingsmaatregelen. Met een pentest kan worden vastgesteld of een informatiesysteem wel of geen gangbare kwetsbaarheden bevat.

### 3.4 Naleving van het beleid

De gemeente vult het beleid in de praktijk in met de volgende producten en acties.

- Het **Informatieveiligheidsbeleid** vormt samen met het jaarlijkse **privacy- & informatieveiligheidsplan** (PIV-plan) het organisatie brede fundament onder een betrouwbare informatievoorziening op strategisch niveau. De directie stelt jaarlijks het PIV-plan vast. De privacydriehoek (FG, CISO en privacyadviseur) stelt het PIV-plan samen op basis van:
    - De uitkomsten van pentesten en audits, zoals de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) en de IT-audit;
    - De evaluatie van opgetreden datalekken en beveiligingsincidenten;
    - De door de stakeholders ingebrachte tactische en operationele onderwerpen voor de beveiliging van processen waarvoor zij verantwoordelijk zijn;
    - Research en evaluaties over cybersecurity;
    - GAP-analyses van normenkaders zoals Baseline Informatiebeveiliging Overheid (BIO), AVG (privacywet) en de WPG (Wet Politiegegevens);
    - Het jaarlijks opgestelde dreigingsbeeld van het Nationaal Cyber Security Center (NCSC) en de Informatie Beveiligingsdienst (IBD);
    - Geleerde lessen van de incidenten bij andere gemeenten en overheden;
    - Eisen die gesteld zijn aan de dienst- en productlevering door derden zoals DigiD.

- De **directie** zorgt dat de teammanagers adequate maatregelen nemen voor de bescherming van de informatie die onder hun verantwoordelijkheid valt. De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van specifieke beleidsregels die aanvullend zijn op dit strategisch beleid.

- De team**managers** zijn verantwoordelijk voor informatiebeveiliging in de processen waarvoor zij verantwoordelijk zijn, inclusief afspraken met (keten)partners. De beveiligingsmaatregelen worden bepaald op basis van risicomanagement; de bedrijfskritische processen krijgen prioriteit. De teammanagers zorgen voor zowel risico-analyses voor het gebruik van processen en de mate van informatiebeveiliging die daarbij nodig is als de controle op het rechtmatig gebruik van de informatie en persoonsgegevens door de medewerkers die de processen uitvoeren. Managers zorgen 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.

- **Medewerkers** moeten verantwoord omgaan met persoonsgegevens en andere gevoelige informatie en daarvoor is kennis en risicobewustzijn van informatiebeveiliging en privacybescherming nodig. Omdat medewerkers (onbedoeld) beveiligingsincidenten kunnen veroorzaken, worden alle medewerkers van de gemeente getraind in het toepassen van informatiebeveiliging in hun dagelijks werk, zoals het aanvaardbaar gebruik van bedrijfsmiddelen. Daarnaast stelt dit eisen aan de gebruiksvriendelijkheid van de ingerichte beveiliging.

- De **CISO** ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en het hierover halfjaarlijks rapporteren aan de directie.

### 3.5 Onderliggend beleid en richtlijnen

Dit beleid is op tactisch en operationeel niveau aangevuld met specifieke beleidsregels. Jaarlijks wordt het onderliggende beleid geëvalueerd en zo nodig bijgesteld. De evaluatie gebeurt zoveel mogelijk aan de hand van bestaande normen en kaders die (inter)nationaal gelden zijn, zodat maatwerk zo min mogelijk nodig is. De openbare beleidsdocumentatie voor informatiebeveiliging is voor iedere medewerker toegankelijk op het gemeentelijke intranet.

### 3.6 Afwijkingen van beleid en regelgeving

De implementatie van beveiligingsmaatregelen kost in sommige gevallen veel geld en capaciteit van de organisatie. Omdat dit schaarse middelen zijn, kan het voorkomen dat bepaalde maatregelen niet of later worden geïmplementeerd. Voor dergelijke afwijkingen kan de teammanager een advies voorleggen aan de directie. De CISO kan hierin ondersteunen. Bij structurele afwijking van verplichte maatregelen dient de directie een besluit te nemen hoe de organisatie met het risico wil omgaan. Geaccepteerde risico’s worden jaarlijks gerapporteerd aan het College van B&W.

Het desbetreffende team zorgt ervoor dat de besluitvorming rond deze afwijkingen goed gedocumenteerd wordt en voor audits toegankelijk is.

# 4. Organisatie, taken en verantwoordelijkheden

### 4.1 Leiderschap en gedrag

Het voorbeeldgedrag en leiderschap van het management is voor informatiebeveiliging van wezenlijk belang – *The Tone at the Top*. Alleen als het management van hoog tot laag zelf laat zien dat informatiebeveiliging belangrijk is, tonenmedewerkers dat gedrag ook . Daarnaast is het belangrijk dat de gemeente een open organisatiecultuur nastreeft, zodat het vertrouwen er is om risico's en incidenten zo snel mogelijk te melden (*Je bent een held als je meldt*) en kennis uit te wisselen. Dit kan gekoppeld worden aan de gloeilamp vanuit de organisatie ontwikkelingen leren & ontwikkelen.

Om informatiebeveiliging binnen de organisatie in te bedden moet aandacht zijn voor:

- processen en ketens binnen de gemeentelijke organisatie,
- cultuur, attitude en gedrag,
- samenwerking, verantwoordelijkheden en bevoegdheden,
- Persoonlijk leiderschap en eigenaarschap.

### 4.2 Governance en eigenaarschap

Om ervoor te zorgen dat de uitgangspunten worden nageleefd en de actiepunten uit de 'jaarplannen privacy en informatieveiligheid'worden uitgevoerd, is het belangrijk om taken, verantwoordelijkheden en bevoegdheden juist te beleggen en daaruit de rollen te destilleren. Iedereen die voor de gemeente werkt is verantwoordelijk voor het beveiligen van informatie en het uiterst zorgvuldig omgaan met informatie (oa. Persoonsgegevens, etc.). In de organisatie hebben een aantal medewerkers een extra verantwoordelijkheid voor informatiebeveiliging. Er moet gezorgd worden voor de uitvoering van het beleid en toezicht dat het op de juiste wijze wordt gedaan. De volgende rollen zijn belangrijk op het gebied van informatiebeveiliging:

- de gemeenteraad
- het College van B&W
- directie
- lijnmanagement (teammanagers)
- concerncontroller
- Chief Information Security Officer (CISO)
- Security Officer (Suwinet).

Omdat informatiebeveiliging in nauwe samenwerking is met privacy, worden hier ook de privacyrollen worden meegenomen. Het is voornamelijk van belang de relatie tussen de verschillende rollen te verhelderen.

- Functionaris gegevensbescherming
- Privacy-adviseur

#### Het College van B&W en gemeenteraad

Binnen de gemeente berust de formele verantwoordelijkheid voor informatiebeveiliging bij het College. Het College van B&W neemt kennis van het informatieveiligheidsbeleid en stelt het vast. Eén van de wethouders is de portefeuillehouder en is daarmee ook eindverantwoordelijk voor het goed beveiligen van de gemeentelijke informatie. Door middel van het hoofdstuk informatieveiligheid in het jaarverslag en de uitkomsten van ENSIA in de collegeverklaring legt het College verantwoording af aan de gemeenteraad over informatieveiligheid.

**Directie**

De directie speelt een cruciale rol bij het uitvoeren van dit strategische Informatieveiligheids-beleid. Enerzijds door richting te geven aan de beveiliging van de informatievoorziening en daarvoor de benodigde middelen beschikbaar te stellen. Daarnaast door binnen de gemeentelijke organisatie uit te dragen dat zij informatiebeveiliging ondersteunt en naleving van het Informatieveiligheidsbeleid bewaakt en handhaaft.

**Teammanagement**

Van het management wordt verwacht dat zij ruimte en tijd bieden aan hun medewerkers om verandering op het gebied van informatiebeveiliging door te voeren. Daarnaast moeten ze bewustwording op het gebied van informatiebeveiliging en privacy promoten. Informatiebeveiliging is niet iets vrijblijvends, het hoort bij de dagelijkse werkzaamheden en moet gedaan worden. De teammanager is verantwoordelijk voor de dataveiligheid van de processen die zich binnen dit team plaatsvinden. Dat geldt ook voor SAAS- en webapplicaties zoals bijvoorbeeld DigiD. De teammanager is de (data-)eigenaar van die processen.

**Concerncontroller**

De concerncontroller is op organisatieniveau verantwoordelijk voor de interne controle op het naleven van het gemeentelijke (informatieveiligheids)beleid. De controller is verantwoordelijk voor het proces van planning en control binnen een organisatie. De controller ziet als onderzoeker toe op de efficiëntie en effectiviteit van de ondernomen activiteiten en adviseert de directie van de organisatie.

**Chief Information Security Officer (Coördinator informatieveiligheid)**

De CISO is verantwoordelijk voor het opstellen en de uitvoering van het beleid. De CISO moet taken uitzetten en bewaken dat er actie ondernomen wordt. Op het moment dat er zich een incident voordoet gaat de CISO aan de slag om het incident te verhelpen. De juiste maatregelen moeten getroffen worden, zodat herhaling in de toekomst voorkomen kan worden.

**Security Officer (Suwinet)**

Op het gebied van Suwinet is een Security Officer aangesteld. De Security Officer houdt zich specifiek op het gebied van Suwinet bezig met informatiebeveiliging. Hierbij hoort het uitzetten van het beleid, medewerkers bewust maken, maar ook de controle op het juist gebruik van Suwinet.

**Medewerkers**

Medewerkers zijn verantwoordelijk voor de dagelijkse omgang met informatiebeveiliging. Zij moeten op de hoogte zijn van de regels. Van hen wordt verwacht dat ze de regels naleven en eventuele incidenten melden via de daarvoor ingerichte procedure.

Ook de mensen die taken hebben die specifiek te maken hebben met informatiebeveiliging of het verbeteren daarvan, moeten zich houden aan de regels. Van hen wordt verwacht dat ze de taken ten aanzien van informatiebeveiliging zo goed mogelijk oppakken en uitdragen richting de collega's.

**Functionaris Gegevensbescherming**

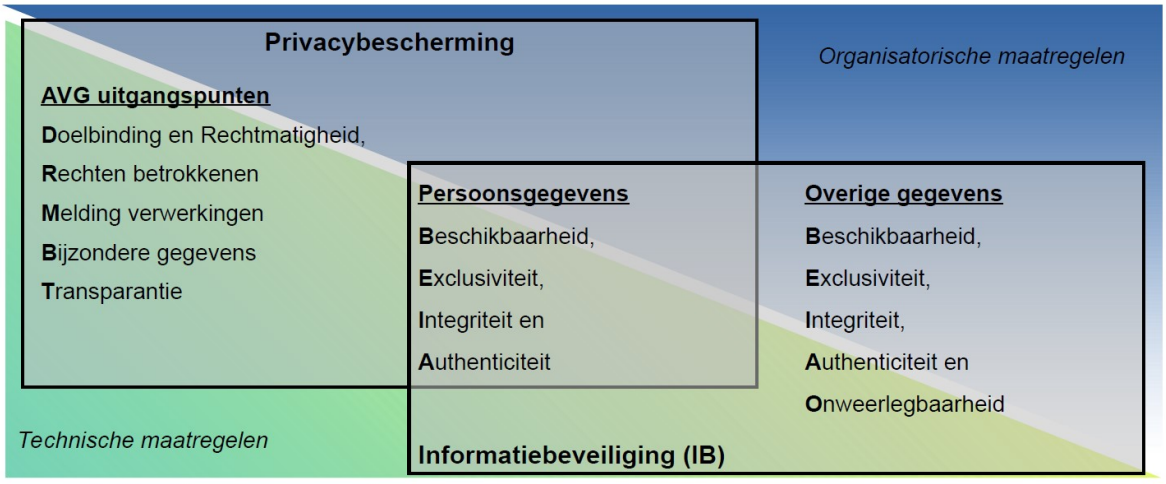
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op het gebied van privacy en houdt toezicht op de verwerking en bescherming van persoonsgegevens. De FG houdt toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast handelt de FG vragen en klachten af van mensen binnen en buiten de organisatie en ondersteunt bij het adviseren over privacy. De FG is contactpersoon van de Autoriteit Persoonsgegevens (AP). De CISO, PA's en FG werken nauw met elkaar samen.

**Privacy Adviseurs**

Binnen gemeente De Ronde Venen zijn naast een FG ook Privacy Adviseurs (PA's) aangesteld. Zij houden zich dagelijks bezig met de uitvoering van het privacybeleid. De PA's brengen de verwerkingen van persoonsgegevens en de privacyrisico's hiervan in kaart, sluiten verwerkersovereenkomsten en hebben een adviserende rol richting de vakafdelingen. Ook nemen de PA's, samen met de CISO, deel aan het datalek- en incidentenproces.

### 4.3 Processen en ketens

Eerder is al aangegeven dat zorgvuldige omgang met de informatie van de gemeente een belangrijke randvoorwaarde is om de dienstverlening verder te kunnen digitaliseren. Informatiebeveiliging moet een integraal onderdeel zijn van de processen binnen de gemeente. Voor de primaire en ondersteunende (PIOFACH) processen ligt die verantwoordelijkheid bij de directie en de teammanagers. Dit start bij het helder beleggen van taken, verantwoordelijkheden en bevoegdheden van managers en medewerkers.
Veel processen bij de Gemeente De Ronde Venen verwerken persoonsgegevens. Bij de beveiliging van deze processen moet een koppeling worden gemaakt met privacybescherming. Het overzicht hieronder toont verschillen en overeenkomsten tussen informatiebeveiliging en privacybescherming.



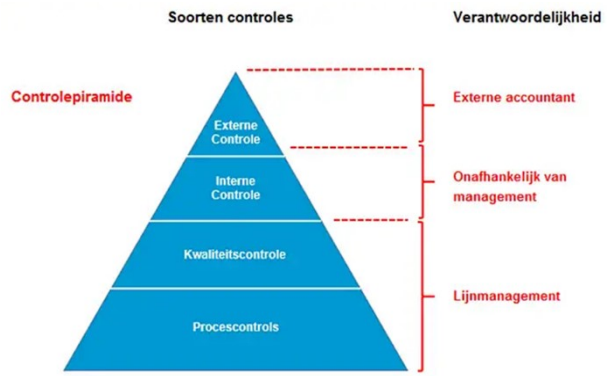

De gemeentesecretaris heeft de verantwoordelijkheid voor toezicht op de informatiebeveiliging gedelegeerd aan de Chief Information Security Officer (CISO). Deze CISO treedt hierbij op als onafhankelijke adviseur van de directie, college, managers en medewerkers.

### 4.4 Kennis, vaardigheden en risicobewustzijn

Het management stelt medewerkers in staat om hun verantwoordelijkheid te nemen voor het beschermen van de informatie van de gemeente. Naast kennis en vaardigheden zijn gedrag, attitude en risicobewustzijn van medewerkers essentieel om dat resultaat te bereiken. Het management streeft naar een organisatiecultuur waarin het vanzelfsprekend is- dat medewerkers hun verantwoordelijkheid nemen om risico's en de incidenten te melden.
Het risicobewustzijn van eigen medewerkers blijft de verantwoordelijkheid van elke manager. Het is echter noodzakelijk dat alle medewerkers de juiste instelling hebben ten aanzien van informatiebeveiliging. Attitude en gedrag zullen daarom op het niveau van de gehele organisatie periodiek aandacht moeten krijgen om medewerkers bewust te houden van de risico's van informatiebeveiliging en binnen de context van hun functie. Op deze manier wordt het juiste gedrag bevorderd en ontstaat een cultuur waarin men elkaar aanspreekt op fout en goed gedrag.

De CISO organiseert organisatiebrede educatie, trainingen en bewustwordingscampagnes. Daarnaast zorgt de CISO met events en publicaties voor continue aandacht voor informatiebeveiliging voor verschillende doelgroepen. Door de overlap van informatiebeveiliging met privacy / gegevensbescherming, zullen initiatieven voor bewustwording gezamenlijk worden georganiseerd.

### 4.5 Samenwerking, verantwoordelijkheden en bevoegdheden




Conform het 3-lijnsmodel is de organisatie van informatiebeveiliging ingedeeld op 3 niveaus: Strategisch, Tactisch en Operationeel, die functioneel naadloos op elkaar moeten aansluiten. De besturing van informatiebeveiliging binnen de gemeente is daarom als volgt ingericht:

- **Strategisch (3e lijn):** team Concerncontrol

  Dit is team Concerncontrol met daarin de kern van de onafhankelijke gemeentelijke informatiebeveiligings-organisatie voor de coördinatie en aansturing bestaande uit de CISO. Door de onafhankelijke positie die team Concerncontrol heeft, is ook geborgd dat informatiebeveiliging en de toetsing hiervan niet beïnvloed wordt door andere belangen en/of overwegingen die binnen de gemeente bij besluitvorming een rol spelen . Hierdoor kan het beeld over informatiebeveiliging binnen de gemeente worden gebruikt in de onafhankelijke verantwoording naar het College, de raad en naar externe partijen.

- **Tactisch (2e lijn):** Adviseurs ondersteuning.

  Vanuit de 2e lijn vervult de (C)ISO de rol van bedrijfsvoeringadviseur voor informatie-beveiliging voor clusters. De (C)ISO ondersteunt de clusters bij het inzichtelijk maken van risico's en advies over toe te passen maatregelen in lijn met de informatiebeveiligings-beleidskaders.

- **Operationeel (1e lijn):** lijnmanagement.

  Voor de veilige verwerking van informatie in de eigen processen kan de teammanager gebruik maken van functioneel en technisch beheerders. Deze beheerders leveren specialistische kennis op diverse vraagstukken zoals: naleving wet- en regelgeving, incidentenonderzoek en -afhandeling, logging en monitoring, netwerkbeveiliging, toegangsbeveiliging en ontwikkeling en beheer van informatiesystemen.
  De teammanager kan ook ondersteuning vragen bij de bedrijfsvoeringsadviseurs. Binnen de context van dit beleid betreft het de afhandeling van security incidenten en risico's.

# Bijlage 1 - verklaring gebruikte afkortingen

| Afkorting | Betekenis |
|---|---|
| ACIB | Algemene Contactpersonen Informatiebeveiliging bij de IBD |
| AVG | Algemene Verordening Gegevensbescherming |
| AP | Autoriteit Persoonsgegevens |
| BCM | Business Continuity Management (bedrijfscontinuïteit) |
| BIO | Baseline Informatiebeveiliging Overheid |
| BRP | Basisregistratie personen |
| CERT | Computer Emergency Response Team (in ons geval de IBD) |
| CIP | Centrum voor Informatiebeveiliging en privacybescherming |
| CISO | Chief Information Security Officer / Coördinator Informatieveiligheid |
| DigiD | Digitale persoonsidentificatie |
| DPIA | Data Protection Impact Assessment (Gegevensbeschermingeffectbeoordeling) |
| DMT | Directie Management Team |
| ENSIA | Eenduidig Normenkader Single Information Audit |
| FG | Functionaris Gegevensbescherming |
| IBD | Informatiebeveiligingsdienst, onderdeel van de VNG |
| ISMS | Information Security Management System |
| NCSC | Nationaal Cyber Security Centrum |
| PA/PO | Privacy Adviseur / Privacy Officer |
| PUN | Paspoortuitvoeringsregeling |
| PNIK | Paspoorten en Nederlandse identiteitskaarten |
| SAAS | Software as a Service |
| Nnb | Nog nader bepalen |
| SUWI | Structuur Uitvoering Werk en Inkomen |
| VCIB | Vertrouwde contactpersonen Informatiebeveiliging bij de IBD |
| VIAG | Vereniging van Informatie- en Automatiseringsprofessionals in Nederlandse Gemeenten |
| VNG | Vereniging van Nederlandse Gemeenten |
| WPG | Wet politiegegevens |

# Bijlage 2 - Functiematrix informatieveiligheid

| rollen/taken in beveiligingsorganisatie | team | huidige medewerker | Plv / tweede |
|---|---|---|---|
| Coördinator informatieveiligheid (CISO) (VCIB) | Concerncontrol | Patrick Zuiderwijk | |
| Controller informatiebeveiliging | Directie | Monique Treur | |
| Beveiligingsbeheerder Basis Registratie Personen | KCC-burgerzaken | Iris Krouwel | Ans Helling |
| Informatiebeheerder Basis Registratie Personen | KCC-burgerzaken | Iris Krouwel | Ans Helling |
| Beveiligingsbeheerder SUWI | K&M welzijn | Sjoerd Buwalda | Vincent Staat |
| Beveiligingsbeheerder BAG | BOR | Marcel Brugman | |
| Beveiligingsbeheerder BGT | BOR | Adrie de Haan | |
| Beveiligingsbeheerder BRO | BOR | Oscar Vergne | Marcel Brugman |
| Functionaris Gegevensbescherming | Concerncontrol | Rob van Gelderen | |
| Privacy-adviseur | JZ | Gert-jan Bremer | |
| Data-eigenaar DigiD, Burgerzaken | KCC-burgerzaken | Mé Benseddik | Hans van Leeuwen |
| Data-eigenaar DigiD, Zaaksysteem | I&A | Marjon Miggels | Chantal Brundel |
| IBD ACIB | I&A | Robert Jan van Santen | Niels de Ruiter |
| IBD VCIB | I&A | Joost Erftemeijer | Richard van Valderen |
| Certificaatbeheer organisatorisch | I&A | Richard van Valderen | Hans Donders |
| Certificaatbeheer functioneel | I&A | Hans Donders | Robert Jan van Santen |
| Uitwijkcoördinator team Automatisering | I&A | Joost Erftemeijer | Richard van Valderen |

Wijzigingen in deze organisatie zullen via de jaarlijkse privacy- en informatieveiligheids-rapportage worden herzien en opnieuw vastgesteld.

==== einde document ====