gemeente roerdalen

# GEMEENTEBLAD

Officiële uitgave van de gemeente Roerdalen

Nr. 187103

21 juli

2020

## Beleidsregel van het college van burgemeester en wethouders van de gemeente Roerdalen houdende regels omtrent strategische informatiebeveiliging 2020-2023

Vastgesteld op: 30 juni 2020 door het college van burgemeester en wethouders van gemeente Roerdalen

### 1. Inleiding

Dit strategische informatiebeveiligingsbeleid geldt voor de jaren 2020 tot 2023 en vervangt het in 2017 vastgestelde informatiebeveiligingsbeleid van GR Servicecentrum MER en de deelnemende gemeenten.

In 2013 hebben gemeenten zich geconformeerd aan de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'. Hierbij is afgesproken om een samenhangend pakket van maatregelen te implementeren om de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en andere informatie(systemen) te waarborgen.

Met dit "Strategisch Informatiebeveiligingsbeleid 2020-2023" zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en informatie(systemen) binnen de gemeente verder te professionaliseren.

Voor dit strategisch informatiebeveiligingsbeleid is ter inspiratie het voorbeeld strategisch informatiebeveiligingsbeleid van de Informatiebeveiligingsdienst (IBD) gebruikt. De andere deelnemende gemeenten van GR Servicecentrum MER en SC MER zelf hebben hetzelfde voorbeeld in hoofdlijnen overgenomen in het lokaal strategisch informatiebeveiligingsbeleid.

Het is een wens van de gemeentesecretarissen dat alle organisaties dezelfde kwaliteitseisen hebben. Het gebruik van het informatiebeveiligingsbeleid van de IBD draagt hieraan bij. Het informatiebeveiligingsbeleid van elke gemeente wordt binnen de eigen interne organisatie vastgesteld. Voor het informatiebeveiligingsbeleid van SC MER geldt dat de moedergemeenten dit beleid eerst laten toetsen op inhoud door het lokale managementteam alvorens dit wordt vastgesteld door het managementteam van SC MER. Dit laatste is ook een wens van de gemeentesecretarissen.

### 1.1 Doel

Dit strategisch informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen. Hiermee zijn informatie, (persoons)gegevens en de verwerking hiervan in goede handen. Daarmee voldoet de gemeente aan relevante wet- en regelgeving.

Dit doel wordt bereikt door:

- de organisatie rondom de informatiebeveiliging op te zetten en te borgen
- risico's van menselijk gedrag te minimaliseren met behulp van bewustwordingscampagnes
- processen en informatie(systemen) te classificeren en vereiste beheersmaatregelen te implementeren
- processen en informatiesystemen in te richten om ongeautoriseerde toegang te voorkomen
- persoonsgegevens van burgers en medewerkers te beschermen en correct te verwerken
- adequaat te reageren op incidenten
- de naleving van dit beleid te borgen

### 1.2 De relatie met de gemeentelijke missie

De inwoners van gemeente Roerdalen moeten er op kunnen vertrouwen dat hun gegevens in goede handen zijn. De aandacht voor informatiebeveiliging groeit. Daarbij heeft de gemeente te maken met *toenemende wet- en regelgeving*. Voor gemeente Roerdalen betekent deze toename van wet- en regelgeving *extra inzet, aanpassen van werkprocessen* en *zorgen voor bewustwording* over het belang van informatiebeveiliging. Hierbij wordt gestreefd naar deregulering. *Dereguleren* betekent voor informatiebeveiliging niet per definitie minder regels, maar begrijpelijke regels en een pragmatische manier van werken *(Bron: Kadernota 2020).*

Ook voor informatiebeveiliging is "*Samen Doen"* het vertrekpunt. Een succesvolle implementatie van informatiebeveiliging hangt af van de *kracht van de medewerkers, zowel individueel als collectief*. Medewerkers moeten worden betrokken zodat zij ook makkelijk initiatief kunnen nemen. Deze betrok-

kenheid is pas optimaal als de medewerkers beseffen waarom informatiebeveiliging belangrijk is. Wij doen dit voor de *inwoners (Bron: Coalitieprogramma 2018-2022).*

De bedrijfsvoering rondom informatiebeveiliging moet net zoals de dienstverlening een *investering* krijgen in *kwaliteit*. Door voor informatiebeveiliging de lat elk jaar een stapje hoger te leggen kan een bijdrage worden geleverd aan een continu betere kwaliteit. Gemeente Roerdalen streeft naar een organisatie die *dicht bij de praktijk* staat, waar *verantwoordelijkheden zo laag mogelijk* in de organisatie worden belegd, zodat de medewerkers *autonoom* kunnen werken. Het inrichten van een organisatie met accenthouders (decentrale informatiebeveiliging en privacy organisatie ) draagt hieraan bij *(Bron: Kadernota 2020).*

Ook wil de gemeente steeds meer zaken aan de burger zo veel mogelijk *digitaal en hiermee plaats- en tijdonafhankelijk* aanbieden. Hoe meer zaken digitaal gaan, hoe meer eisen er gesteld worden aan stabiliteit, betrouwbaarheid, veiligheid en kwaliteit van de digitale informatiestromen. Er is informatieuitwisseling tussen gemeente en inwoners, maar ook tussen overheden of tussen gemeenten en professionele organisaties. Dit heeft invloed op de informatiebeveiliging *(Bron: Kadernota 2020).*

### 1.3 Leeswijzer

In hoofdstuk 2 van dit beleid is het ambitieniveau rondom informatiebeveiliging beschreven. Dit is de stip op de horizon en bepaalt de keuzes die gemaakt moeten worden. De kern van het strategisch beleid staat in hoofdstuk 3. Hoofdstuk 4 beschrijft vervolgens hoe de rollen, taken en verantwoordelijkheden in de organisatie belegd zijn.

## 2. Ambitie Informatiebeveiliging

Het profiel en de ambitie van de gemeente Roerdalen geeft de koers weer en is richtinggevend en bepalend voor de informatievoorziening en hiermee de informatiebeveiliging.
Informatiebeveiliging maakt momenteel nog geen onderdeel uit van de dagelijkse besluitvorming. De ambitie van gemeente Roerdalen rondom informatiebeveiliging is een stapsgewijze groei. Door een organisatie te laten groeien in stappen, kan de omslag worden teruggebracht tot een reeks van kleine veranderingen en realistische doelen.
Het huidige volwassenheidsniveau van gemeente Roerdalen, geclassificeerd conform het volwassenheidsmodel NBA-LIO/NOREA (versie januari 2019)[1], ligt tussen niveau 1 en 2. De ambitie is om in 2020 te groeien naar een niveau tussen 2 en 3. Om te kunnen voldoen aan wet- en regelgeving én hierbij risico's te beperken tot acceptabel niveau is minimaal een volwassenheidsniveau van 3 nodig[2]. Op dit niveau kan worden aangetoond dat informatiebeveiliging is geborgd in de werkprocessen (opzet, bestaan en werking).

De gemeente streeft haar visie na en wil niet middelmatig blijven. De ambitie hierbij is om te groeien naar een volwassenheidsniveau tussen 3 en 4 in 2024. Zodra de volwassenheid van de organisatie op niveau 4 is, heeft de organisatie voldoende kennis om proactief op ontwikkelingen in de werkprocessen te anticiperen. Dit naast het uitvoeren van de zelfevaluaties en de borging van de bestaande beheersmaatregelen in werkprocessen.

Noodzakelijke randvoorwaarde om deze groei te bereiken is de beschikbaarheid van middelen binnen de teams. Met de inrichting van een decentrale informatiebeveiliging en privacy organisatie (accenthouders) is al een grote eerste stap gezet. Met deze inrichting groeit de gemeente vanuit organisatieonderdelen en kan integraal worden gewerkt aan het verbeteren van de informatiebeveiliging. Hierin is gemeente Roerdalen afhankelijk van de kwaliteit van de dienstverlening van SC MER.

In tabel 1 op de volgende pagina's is in de laatste kolom concreet gemaakt wat er moet gebeuren om te groeien van het ene niveau naar het ander niveau. Dit overzicht is niet uitputtend. Er zijn ook andere, voornamelijk ICT gerelateerde, thema's die geen plek hebben gekregen in deze tabel. Hierdoor blijft dit informatiebeveiligingsbeleid leesbaar en wordt voorkomen dat het te technisch wordt.

| Niveau | Naam | Omschrijving | Indicatieve criteria | Wat moet hiervoor gebeuren? |
|---|---|---|---|---|

1) *NBA-LIO is de beroepsorganisatie voor accountants. NOREA is de beroepsorganisatie voor IT-auditors. Het volwassenheidsmodel is gemaakt in samenwerking tussen deze beroepsorganisaties.*
2) *IT-auditors gaan naast opzet en bestaan meer letten op werking. Er is pas sprake van werking bij volwassenheidsniveau 3.*

| | | | | |
|---|---|---|---|---|
| 1 | Initieel | Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen. | - Geen of beperkte controls geïmplementeerd.<br>- Niet of ad-hoc uitgevoerd.<br>- Niet /deels gedocumenteerd.<br>- Wijze van uitvoering afhankelijk van individu. | |
| 2 | Herhaalbaar | Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd. | - Control is geïmplementeerd.<br>- Uitvoering is consistent en standaard.<br>- Informeel en grotendeels gedocumenteerd. | - Definiëren van het strategisch en tactisch beleid.<br>- Er is een informatiebeveiligingsplan gedefinieerd.<br>- Kritische rollen zijn gedefinieerd en toegewezen.<br>- Er is beleid voor risicomanagement binnen informatiebeveiliging gedefinieerd. Wordt gebruikt bij grote projecten of bij incidenten.<br>- Er is een proces voor trainingen en opleidingen.<br>- Classificatie van informatie gebeurt informeel en adhoc. |
| 3 | Gedefinieerd | Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. | - Control gedefinieerd o.b.v. risicoassessment.<br>- Gedocumenteerd en geformaliseerd.<br>- Verantwoordelijkheden en taken eenduidig toegewezen.<br>- Opzet, bestaan en effectieve werking aantoonbaar.<br>- Rapportage van uitvoering van beheersingsmaatregel aan management.<br>- Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie.<br>- De toetsing toont aan dat de control effectief is. | - Goedkeuren strategisch en tactisch informatiebeveiligingsbeleid en het intern en extern delen van dit beleid.<br>- Het informatiebeveiligingsplan is goedgekeurd en vertaald naar concrete acties met hierbij de juiste inzet van middelen.<br>- Alle rollen zijn gedefinieerd en toegewezen. De (eind)verantwoordelijkheden zijn ook vastgelegd voor afdelingsoverstijgende onderdelen.<br>- Er is organisatiebreed beleid voor risicomanagement en vastgesteld. Beleid en processen besteden aandacht aan de essentiële[3] onderdelen van risicomanagement. Het beleid ligt in lijn met het algemeen beleid risicomanagement.<br>- Processen voor trainingen en opleidingen zijn geïmplementeerd en worden uitgevoerd. Opleidingen en trainingen worden gebruikt om te verifiëren of iemand de juiste competenties heeft om een rol te vervullen.<br>- Er is vastgesteld beleid en hieruit voortvloeiende processen voor de classificatie van data. |

3) *Risicoprofiel, risicobereidheid, eigenaarschap, risico assessment, risico mitigeren, risico acceptatie*

| | | | | |
|---|---|---|---|---|
| 4 | Beheerst en meetbaar | De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd. | - Periodieke (control) evaluatie en opvolging vindt plaats.<br>- Evaluatie is gedocumenteerd en geformaliseerd.<br>- Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks.<br>- Rapportage van de evaluatie aan management. | - Het strategisch beleid dient als kapstok voor alle acties rondom informatiebeveiliging.<br>- Het strategisch en tactisch beleid worden periodiek gecontroleerd op naleving.<br>- Het tactisch beleid is vertaald in operationeel beleid en richtlijnen.<br>- Het plan is/wordt (gefaseerd) geïmplementeerd. Er is hiernaast ook een proces voor het periodiek evalueren en updaten van het plan.<br>- Eigenaarschap, rollen en (eind)verantwoordelijkheden worden periodiek geëvalueerd.<br>- Het kader voor risicomanagement en de effectiviteit hiervan wordt periodiek geëvalueerd en hierover wordt gerapporteerd.<br>- Periodiek wordt getoetst of op een juiste en volledige wijze data is geclassificeerd. |
| 5 | Continu verbeteren | De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering. | - Cntinu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit zelfassessment, gap en root cause analyses.<br>- De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties.<br>- Real time monitoring.<br>- Inzet automated tooling. | - M.b.t. compliance wordt periodiek gerapporteerd aan het hoger management.<br>- Het informatiebeveiligingsplan wordt periodiek gemonitord op progressie, bedreigingen, haalbaarheid etc.<br>- Risicomanagement is geïntegreerd in alle bedrijfs- en IT-processen.<br>- Jaarlijks worden de processen en de inhoud van trainingen en opleidingen geëvalueerd. |

*Tabel 1 Volwassenheidsniveau (Bron: volwassenheidsmodel NBA-LIO/NOREA, versie januari 2019)*

## 3. Beleidskader Informatiebeveiliging

### 3.1 Plaats van dit beleid

Dit beleid is een onderdeel van het informatiebeveiligingsbeleid dat wordt vertaald in tactische en operationele uitgangspunten en maatregelen. Dit strategisch beleid dient als kapstok en is een algemene basis. De uitwerking van dit beleid staat opgenomen in het jaarlijks vast te stellen informatiebeveiligingsplan. Het plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.

Onderdeel van het informatiebeveiligingsbeleid zijn:
- onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau
- procedures en werkinstructies op operationeel niveau
- de acties en planning die nodig zijn om te voldoen aan dit beleid

Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen[4]. Hiervoor gelden specifieke informatiebeveiligingsplannen.

4) *Zoals Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK), Digitale Identiteit (DigiD), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO)*

### 3.2 Scope
Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, organisatieonderdelen, objecten, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Om er voor te zorgen dat bij externe partijen alles volgens onze norm en kwaliteitseisen gebeurt worden afspraken gemaakt met ketenpartners. Dat gebeurt bijvoorbeeld in de inkoopvoorwaarden, verwerkersovereenkomst of d.m.v. een Third Party Memorandum (TPM).

Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politiek bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

### 3.3 Grondslagen
Dit strategisch informatiebeveiligingsbeleid is gebaseerd op internationale standaarden voor informatiebeveiliging zoals NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Hiernaast is dit strategisch informatiebeveiligingsbeleid gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO)[5] en afgeleid van bovenstaande NEN-normen, aangevuld met de 10 principes voor informatiebeveiliging (zie 3.4.2) zoals uitgewerkt door de VNG. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

### 3.4 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid staan hieronder opgenomen. Naast de nieuwe Baseline Informatiebeveiliging Overheid (BIO) en de "10 principes voor informatiebeveiliging" worden ook de ontwikkelingen uit het jaarlijkse "Dreigingsbeeld Nederlandse Gemeenten" gevolgd.

#### *3.4.1 De BIO*
De BIO is vanaf 2020 het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude Baseline Informatiebeveiliging Gemeenten (BIG). Doordat er meer focus is op risicomanagement betekent het dat bij medewerkers de verantwoordelijkheid begint met een prominente rol voor teamleiders. Hierbij maakt het management op voorhand keuzes en continu afwegingen ten aanzien van het niveau van passende beveiliging, de implementatie van passende risicoverlichtende maatregelen en acceptatie van de risico's die daarna nog resteren.

#### *3.4.2 De 10 principes voor informatiebeveiliging*
De 10 principes voor informatiebeveiliging[6] zijn een bestuurlijke aanvulling op de BIO. De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. De VNG adviseert om deze principes te gebruiken omdat deze de bestuurder ondersteunen bij het uitvoeren van goed risicomanagement. Indien er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente, daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

De principes zijn als volgt:
1. Bestuurders bevorderen een veilige cultuur;
2. Informatiebeveiliging is van iedereen;
3. Informatiebeveiliging is risicomanagement;
4. Risicomanagement is onderdeel van de besluitvorming;
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. Informatiebeveiliging is een proces;
7. Informatiebeveiliging kost geld;
8. Onzekerheid dient te worden ingecalculeerd;
9. Verbetering komt voort uit leren en ervaring;
10. Het bestuur controleert en evalueert.

5) *Uitgebracht door de interbestuurlijke werkgroep Normatiek in 2018: Deze werkgroep bestaat uit vertegenwoordigers van o.a. VNG en de IBD, waterschappen, provincies en het rijk.*

6) *Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)*

### *3.4.3 Dreigingsbeeld Nederlandse Gemeenten*
Het dreigingsbeeld Nederlandse Gemeenten geeft jaarlijks een actueel zicht op incidenten en factoren uit het verleden aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is een bron om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

### *3.4.4 Informatie uit incidenten en inbreuken op de beveiliging*
De gemeente kent naast het hierboven genoemde dreigingsbeeld ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid en plan.

## 3.5 Uitgangspunten
Onze belangrijkste uitgangspunten van het beleid zijn:
1. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament om informatiebeveiliging in de organisatie te borgen.
2. Medewerkers gaan verantwoord om met persoonsgegevens en andere informatie.
3. Het vergroten van het bewustzijn van medewerkers vraagt continue aandacht van het management.
4. Iedere medewerker, zowel vast als tijdelijk, intern of extern beschermt waar nodig gegevens en informatiesystemen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
5. Medewerkers spreken elkaar aan op onveilig gedrag en werken mee om beveiligingsincidenten te voorkomen en de effecten hiervan te beperken.
6. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers kennen de beveiligingsprocedures en passen deze procedures adequaat toe.
7. Informatiebeveiligingstaken zijn binnen de bedrijfsprocessen belegd en de benodigde mensen en middelen zijn beschikbaar gesteld om informatiebeveiliging te borgen volgens dit beleid.
8. Informatiebeveiliging is een integraal onderdeel van risicomanagement.
9. Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging. Door organisatiebrede planning, implementeren van maatregelen, periodieke controle én coördinatie verankert informatiebeveiliging binnen de organisatie.
10. Er is inzicht in welke informatie en informatiesystemen van algemeen belang zijn voor de gemeente en welke informatie van vitaal en kritiek belang is. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor het behalen van de gemeentelijke missie, visie en doelen.

Eventuele tekortkomingen binnen bovenstaande uitgangspunten worden als verbetermaatregel opgenomen in het jaarlijks vast te stellen informatiebeveiligingsplan.

## 4. Organisatie, taken en verantwoordelijkheden

De wijze waarop het informatiebeveiligingsbeleid binnen de gemeente is verankerd, vormt het fundament van de borging van informatiebeveiliging. Het bestuur, de directie en het teammanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid.

In dit hoofdstuk is toegelicht welke rollen, 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 (figuur 1). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO) 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.

| Verdedigingslinie | Waar? | Verantwoordelijkheid |
|---|---|---|
| Eerste lijn | Teamleiders, Accenthouder | Primair verantwoordelijk voor uitvoering en risicobeheersing |
| Tweede lijn | CISO, Privacy Coördinator | Ondersteunt, bewaak en rapporteert. Monitort vanuit een advies- en toetsende rol de risicobeheersing door de eerste lijn |
| Derde lijn | FG | Beoordeelt vanuit een onafhankelijke positie de effectiviteit van de interne beheersing en de werking van de eerste en tweede lijn |

*Figuur 1 Three Lines of Defence (3LoD)*

### 4.1 Gemeenteraad
De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan hen toekent. Dit vormt het zogenaamde horizontaal toezicht.

### 4.2 College van Burgemeester en Wethouders
Het College van Burgemeester en Wethouders is integraal (politiek) verantwoordelijk voor de beveiliging van informatie en de borging van de privacy binnen de gemeentelijke bedrijfsprocessen. Zij stelt kaders op voor informatiebeveiliging en de bescherming van privacy op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Dit stelt het college vast in het informatiebeveiligingsbeleid. In een aantal specifieke bij wet bepaalde gevallen (zoals waardedocumenten) ligt deze bevoegdheid bij de burgemeester in plaats van bij het college. Het college mandateert de ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging en privacy aan de gemeentesecretaris. Zowel het college van Burgemeester en Wethouders als de Raad (controle functie) kunnen opdracht geven om controle te laten uitvoeren.

### 4.3 Directieteams
De directie is ambtelijk verantwoordelijk voor sturing. De gemeentesecretaris draagt de gemandateerde verantwoordelijkheid voor informatiebeveiliging. De gemeentesecretaris stelt samen met de directie het gewenste niveau van informatiebeveiliging. De directie maakt 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 de directie dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

De directie:
- zorgt dat het tactische beleid, het informatiebeveiligingsplan en de operationele procedures worden opgesteld en stelt deze documenten vast.
- adviseert het college van B&W over het vast te stellen strategische beleid.
- stuurt op concern risico's ten aanzien van informatiebeveiliging en privacy en stelt het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast.
- zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider en ziet erop toe dat de teamleiders adequate maatregelen nemen.
- controleert of de getroffen maatregelen overeenstemmen met de gestelde eisen en of deze voldoende bescherming bieden.
- informeert de eindverantwoordelijke portefeuillehouders binnen het College gevraagd en ongevraagd over informatiebeveiliging.
- ziet erop toe dat informatiebeveiligingsonderwerpen n.a.v. de rapportage van de CISO onderdeel zijn van de P&C-voortgangsgesprekken en dat risicovolle onderwerpen worden opgenomen in de auditplannen.

### 4.4 Eerste lijn: Teamleiders
De teamleiders zijn operationeel eindverantwoordelijk. Zij zorgen dat de inrichting van informatiebeveiliging binnen de processen voldoet aan de vereiste wet- en regelgeving. Hierbij worden zij ondersteund vanuit de tweede lijn door de CISO.
Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben, er moet dus altijd iemand verantwoordelijk zijn. Teamleiders rapporteren over de door hun tactisch- en operationeel uitgevoerde activiteiten rondom informatiebeveiliging aan de directie.

Taken van de teamleiders zijn:

- het opstellen, vaststellen en uitdragen van specifiek uitvoeringsbeleid, specifieke reglementen en operationele procedures op hun werkterrein. Hierbij worden zij ondersteund door de tweede lijn.
- de implementatie en uitvoering van de informatiebeveiligingsmaatregelen binnen de processen waarvoor zij verantwoordelijk zijn. Deze beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Om deze risicoafwegingen te kunnen maken wordt gebruik gemaakt van de QuickScans van de BIO.
- het leveren van input voor wijzigingen op maatregelen en procedures.
- het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.

- zorgdragen dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens inzien en verwerken.
- aanleveren van alle informatie die nodig is voor het invullen van de jaarlijkse verantwoordingstraject informatiebeveiliging (ENSIA).
- bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.
- afstemming over de inhoudelijke aanpak van informatiebeveiliging in het bedrijfsvoeringsoverleg met de teams.
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit, privacy en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

Er zijn op deelgebieden beveiligingsbeheerders die de verantwoordelijkheid, bevoegdheid en taak krijgen om de informatiebeveiliging zoveel mogelijk te waarborgen.

### 4.5 Eerste lijn: Accenthouder

De accenthouder draagt zorg voor het beheer, de coördinatie en het advies ten aanzien van de informatiebeveiliging en privacy op zijn/haar deelgebied. Vanuit deze rol zijn deze medewerkers eerste aanspreekpunt voor de CISO en de FG en ambassadeur voor informatiebeveiliging en privacy binnen de organisatie.

De accenthouder monitort of de informatiebeveiliging conform de kaders uitgevoerd wordt. Hij is direct betrokken bij de implementatie hiervan in de lijn en kent de processen en relevante wetgeving. Hij zorgt daarmee dat de organisatie specifieke informatiebeveiliging wordt doorgevoerd in de processen, conform wet- en regelgeving. De accenthouder is deelnemer van de werkgroep ENSIA. De accenthouder is samen met de CISO en de FG, het aanspreekpunt op het gebied van informatiebeveiliging en privacy en bevordert het beveiligingsbewustzijn en draagvlak bij management en medewerkers. De accenthouder rapporteert periodiek over de informatiebeveiliging en privacy aan de teamleider, CISO en FG.

### 4.6 Tweede lijn: Chief Information Security Officer

De Chief Information Security Officer (CISO) is binnen de gemeente degene die kaders stelt op het gebied van informatiebeveiliging. De CISO stuurt de organisatie aan met betrekking tot informatiebeveiliging. Hiermee zorgt hij ervoor dat de organisatie informatiebeveiliging doorvoert in de processen, conform wet- en regelgeving. Daarnaast creëert de CISO het draagvlak voor informatiebeveiliging binnen de organisatie. De CISO is geen hiërarchische maar een inhoudelijke coördinator. De CISO is in het kader van het verantwoordingstraject informatiebeveiliging tevens coördinator ENSIA. De CISO zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De CISO ondersteunt vanuit een onafhankelijke positie de organisatie met betrekking tot het borgen van informatiebeveiliging en rapporteert hierover rechtstreeks aan de directie en/of portefeuillehouder.

### 4.7 Derde lijn: Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) houdt toezicht op de wijze waarop de organisatie invulling geeft aan maatregelen om aan de privacywetgeving te voldoen. In het privacybeleid staan de taken van de FG opgenomen. De artikelen 37, 38 en 39 van de Algemene Verordening Gegevensbescherming (AVG) beschrijven de verplichting, positie en taken van de FG.

### 4.8 ENSIA: Eenduidige Normatiek Single Information Audit [7]

Jaarlijks legt gemeente Roerdalen verantwoording af over de stand van zaken rondom informatiebeveiliging. Dit gebeurt d.m.v. ENSIA. ENSIA bestaat uit een horizontaal en een verticaal verantwoordingstraject.

**7 ) Het project ENSIA was een gezamenlijk project van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het toenmalige ministerie van Infrastructuur & Milieu (I&M) en de Vereniging van Nederlandse Gemeenten (VNG). Het project had tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het project is een resultaat van de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" die in november 2013 tijdens de Buitengewone Algemene Ledenvergadering van de VNG is aangenomen. In deze resolutie hebben de gemeenten het belang van informatieveiligheid erkend en de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) aangenomen als hét gemeentelijk basisnormenkader voor informatieveiligheid. De gemeenten hebben zich gecommitteerd aan de implementatie van de BIG in de eigen organisatie. Daarnaast informeert een college van B&W de gemeenteraad over informatieveiligheid in het jaarverslag. In de resolutie hebben de gemeenten ook een oproep gedaan aan de rijksoverheid en ketenpartners om de verantwoordingslast over informatieveiligheid te verminderen.**

De horizontale verantwoording via het college van B&W richting de gemeenteraad bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het college van B&W en een passage over informatieveiligheid in het jaarverslag. De verticale verantwoording richting het rijk gaat over de BRP en Reisdocumenten, Suwinet, BAG, BGT, BRO en DigiD.

### 4.9 Communicatie van dit beleid

Na vaststelling van het informatiebeveiligingsbeleid wordt dit beleid gecommuniceerd met alle interne en externe stakeholders.