Regionale Sociale Dienst
KROMME RIJN HEUVELRUG

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1250
27 mei
2025

Officiële uitgave van de gemeenschappelijke regeling Regionale Dienst Werk en Inkomen Kromme Rijn Heuvelrug

RSD-Strategisch Informatiebeveiligingsbeleid 2025 – 2027

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid 2025 tot 2027 (IB-beleid) voor de jaren 2025 tot 2027 en vervangt het in 2021 vastgestelde 'Strategisch Informatiebeveiligingsbeleid'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit IB-beleid zet de RSD een volgende stap om de beveiliging van persoonsgegevens en andere informatie te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan (vastgesteld door het managementteam) worden deze tactische en operationele aspecten van informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de unitmanagers, de CISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie. Het informatiebeveiligingsbeleid geldt voor alle processen van de RSD en 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 alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

De RSD verwerkt voor de uitvoering van haar taken (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de RSD voor het goed kunnen uitvoeren van de wettelijke taken. Denk hierbij onder andere aan begeleiding en hulp bij het vinden van werk, het aanvragen van een uitkering, het oplossen van schulden en andere vormen van inkomensondersteuning. Om als sociale dienst deze taken goed uit te voeren is het noodzakelijk om persoonsgegevens te verwerken.

1.4 Ambitie en visie van de RSD op het gebied van informatiebeveiliging en privacy

De RSD hecht grote waarde aan een goede dienstverlening aan haar inwoners en bedrijven op alle vlakken waar de RSD verantwoordelijk voor is. Ook wil de RSD een betrouwbare en transparante partij zijn naar haar inwoners en bedrijven. Hiervoor is het noodzakelijk dat de informatie die wij verzamelen, bijhouden en verwerken en publiceren te allen tijde beschikbaar is, juist en actueel is (integer) en, indien van toepassing, alleen toegankelijk is voor degenen die toegang moeten hebben (vertrouwelijk). De RSD wil meegaan met nieuwe ontwikkelingen en technologie om de dienstverlening verder te verbeteren.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2025 tot 2029. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan. Het beleid op informatiebeveiliging dient ondersteuning te bieden aan het dagelijks bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het IB-beleid zijn de volgende:

2.2.1 De BIO
De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de unitmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitaal wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De RSD is zich hiervan bewust en wil daarom aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG). Dit is vastgelegd in het Privacybeleid van de RSD en aanverwante procedures en richtlijnen.

2.2.3 De Wpg
Wanneer de RSD een sociaal rechercheur in dienst zou hebben en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (Wpg) dan geldt het volgende; hiervoor heeft de RSD Privacy beleid en samenhangende procedures ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

2.2.4 De 10 principes voor informatiebeveiliging[1]
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. 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.
- Verbetering komt voort uit leren en ervaring.
- Het bestuur controleert en evalueert.

Deze principes ondersteunen het dagelijks bestuur en het managementteam (MT) bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de RSD. Redengevend om het onderwerp informatiebeveiliging nadrukkelijk op de agenda van het MT en het dagelijks bestuur te plaatsen.

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.6 Informatie uit incidenten, inbreuken op de beveiliging en datalekken
De RSD kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen.

1) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Voor de ondersteuning van gemeenten en sociale diensten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacy plan zal deze structuur volgen.

Binnen de RSD wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Het beveiligingsbeleid van de RSD is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezighouden.[3] Voor de bescherming van PA gebruikt de RSD de Cybersecurity Implementatie Richtlijn (CSIR).[4]

2.4 Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan'.

2.5 Scope informatiebeveiliging
De scope van deze beleidsnota omvat alle processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de RSD en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

Alle informatie en informatiesystemen zijn van belang voor de RSD, bepaalde informatie is van vitaal en kritiek belang. Het dagelijks bestuur is eindverantwoordelijke voor de informatiebeveiliging. Dit geldt voor alle informatiesystemen ongeacht waar deze worden gehost.

2.6 Uitgangspunten
Het bestuur, het MT en het lijnmanagement spelen een cruciale rol bij het uitvoeren van dit strategische IB-beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de RSD heeft, de risico's die de RSD hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging en ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&-beleid van en voor de hele RSD. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het IB-beleid is in lijn met het algemene beleid van de organisatie en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen
De strategische doelen van het IB-beleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.

2) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.
3) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
4) https://www.cert-wm.nl/csir

- 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 burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de RSD 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 IB-beleid vormt samen met het IB-plan het fundament onder een betrouwbare informatievoorziening. In het IB-plan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De RSD stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het IB-beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig de data van de informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 IB governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het dagelijks bestuur stelt als eindverantwoordelijke het strategisch IB-beleid vast.
- Het MT stelt jaarlijks het IB-plan vast.
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Het MT is verantwoordelijk voor het vragen om informatie bij de unitmanagers en ziet erop toe dat de unitmanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en proces automatiseringssystemen die onder hun verantwoordelijkheid 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 MT, voorafgaand aan de P&C-gesprekken.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO en de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De unitmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De unitmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de RSD. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de RSD en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de RSD worden getraind in het gebruik van beveiligingsprocedures.

- Alle medewerkers hebben een minimale basiskennis van informatiebeveiliging en privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Onder verantwoordelijkheid van de unitmanagers worden quickscans informatiebeveiliging uitgevoerd op basis van de BIO. Bij het verwerken van persoonsgegevens worden tevens (Pre-)DPIA's uitgevoerd uit op basis van de AVG uit om risico-afwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB-plan opgesteld onder leiding van de CISO, gebaseerd op:
  - Dit IB-beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten
  - Het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risico-analyses en DPIA's
  - De door de unitmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB-plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken & verantwoordelijkheden

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 het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging binnen de eigen processen. De tweede lijn (CISO, security officers, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering. Voor een meer gedetailleerde uitwerking van de verantwoordelijkheden per functie verwijzen we naar de binnen de RSD vastgestelde functieprofielen.[5]

3.1 Aansturing: het managementteam

Het MT zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een unitmanager. Het MT zorgt dat de unitmanagers zich verantwoorden over de beveiliging en bescherming van de (persoons)gegevens of andere informatie die onder hen berust. Het MT zorgt dat de eindverantwoordelijke portefeuillehouders binnen het dagelijks bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het dagelijks bestuur zich ook verantwoorden naar het algemeen bestuur.

Het MT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het MT draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacy beleidsonderwerpen en laat zich hierin bijstaan door de CISO, ISO en PO van de RSD. Het MT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de RSD gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: unitmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle unitmanagers. 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

5) De functieprofielen zijn vastgelegd in het document 'RSD-Governancemodel van de informatiebeveiliging & privacyorganisatie'

processen, systemen, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Unitmanagers rapporteren aan het MT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het MT. Voorbereiding en coördinatie van dit overleg ligt bij de CISO.

Taken van de unitmanagers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.
- Het binnen de eigen afdeling uitdragen van het IB-beleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO, ISO en PO bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Rollen en Taken binnen het 3-Lines of Defence model		
1e lijn -> Directie, lijnmanagement, medewerkers	**2e lijn -> CISO en TISO*, samenwerkend in een Information Security-team**	**3e lijn -> Controller, auditor, FG**
Dagelijkse operatie • Voldoen aan beleid • Implementatie beleid • Inrichting processen • Maken werk-beschrijvingen • Inrichting techniek • Risico-eigenaar	**Kader stellend** • Definiëren kader stellend beleid **Adviseren** • Ondersteunen 1e lijn	**Onafhankelijke toetsing van 1e en 2e lijn m.b.t.** • Naleving beleid • Uitvoer processen • De realisatie van de maatregelen • De afhandeling van beveiligingsincidenten
Borging • Borging kennis • 1e lijn controles • Inrichten functiescheiding	**Toetsend** • Dagelijkse operatie toetsen aan beleid • Review operationeel beleid **Monitorend** • Control review • Risico assessment	**Onafhankelijk betekent** • Geen operationele verantwoordelijkheid • Geen beleidsmatige verantwoordelijkheid

	• Risico monitoring	

* Technisch information security officer, ondergebracht bij de GR RID

3.3 Controle en verantwoording

Dit IB-beleid is een verantwoordelijkheid van het dagelijks bestuur van de RSD. Het dagelijks bestuur van de RSD werkt volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Het MT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het MT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.3.1 ENSIA

Ongeacht de delegatie van taken en verantwoordelijkheden op het terrein van werk en inkomen aan de RSD, blijven de deelnemende gemeenten bestuurlijk verantwoordelijk voor het gebruik van Suwinet door de RSD. Deze verantwoording wordt afgelegd in het ENSIA-proces. ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. Dit vindt plaats volgens een vastgesteld verantwoordingsproces van zelfevaluatie naar het opstellen van een collegeverklaring en een externe audit. De RSD heeft een taak en verantwoordelijkheid in het ENSIA-proces richting de deelnemende gemeenten.

4. Financiering van Informatieveiligheid

4.1 Kosten en verdeling

Informatieveiligheid kost geld en zal ook meer gaan kosten aangezien organisaties steeds afhankelijker van ICT worden. Tot op heden worden de kosten van informatieveiligheid grotendeels gedekt vanuit ICT-budgetten. Om meer overzicht te krijgen in de kosten is het noodzakelijk om deze kosten beter in beeld te krijgen. Tegelijkertijd is het logisch dat informatieveiligheid het beste gediend is door de financiering te beleggen bij de betrokken eigenaren.
Voorgesteld wordt de volgende splitsing aan te brengen:

- De kosten van de beveiliging van de IT-infrastructuur komt ten laste van de kostenplaats automatisering.
- De kosten voor de uitvoering van IT-audits en assessments, zoals ENSIA, komen ten laste van de kostenplaats automatisering.
- Personele kosten RSD zitten in de betreffende in unitbudgetten.
- De personele loonkosten van de ISO en de CISO worden door de RID aan de deelnemers doorbelast volgens de afgesproken verdeelsleutel.
- Scholing en kennisopbouw van medewerkers komen voor een deel ten laste van de unitbudgetten en voor een deel ten laste van het organisatie brede opleidingsbudget.