



## **Integriteitsbeleid**

**Stichting Bedrijfstakpensioenfonds voor de Meubelindustrie en  
Meubileringsbedrijven**

**Juni 2018**

# Inhoud

<b>1</b>	<b>Samenhang</b> .....	<b>3</b>
<b>2</b>	<b>Integriteit algemeen</b> .....	<b>6</b>
	<i>Generieke beheersing: HR</i> .....	<i>8</i>
	<i>De internal audit voert periodiek audits uit om de te beoordelen of de eerste lijn en tweede lijn hun verantwoordelijkheden zijn nagekomen ten aanzien van deze recruitment en belonings-processen. Generieke beheersing: governance</i> .....	<i>9</i>
<b>3</b>	<b>Integriteitsthema's</b> .....	<b>11</b>
	<i>Fraude/ corruptie</i> .....	<i>11</i>
	<i>Witwassen</i> .....	<i>12</i>
	<i>Terrorismefinanciering en naleving sanctiewetgeving</i> .....	<i>13</i>
	<i>Belangenverstremgeling/ omkoping</i> .....	<i>14</i>
	<i>Handel voorwetenschap</i> .....	<i>15</i>
	<i>Onethisch handelen</i> .....	<i>16</i>
	<i>Fiscaliteit</i> .....	<i>17</i>
	<i>IT</i> 18	
	<i>Privacy</i> .....	<i>18</i>

## 1 Samenhang

Stichting Bedrijfstakpensioenfondsvoor de Meubelindustrie en Meubileringsbedrijven (hierna 'het pensioenfondsv') heeft een missie, visie, doelstellingen en strategie ontwikkeld.

Het integriteitsbeleid gaat over de manier waarop het bestuur wenst dat het pensioenfondsv handelt en omgaat met elkaar en met de stakeholders. Het bestuur hecht daar grote waarde aan en voert een actief beleid om dit verder te versterken. Er is derhalve een koppeling met missie, visie, doelstellingen en strategie.

### Doel

Het doel is het handhaven van algemene of professionele sociale en ethische normen en waarden waardoor het pensioenfondsv zodanig is georganiseerd dat het integriteitsrisico tot een voor het pensioenfondsv acceptabel niveau is teruggebracht en het pensioenfondsv adequaat kan optreden tegen eventuele incidenten.

### Definitie, Beleid & Three lines of defence

Vanuit het oogpunt "in control" dient het pensioenfondsv haar structuur zodanig vorm te geven dat het bestuur aantoonbaar in staat is om de bestuurlijke eindverantwoordelijkheid te dragen inzake de naleving van de diverse beleidsterreinen waaronder integriteit. Het bestuur stelt in eerste instantie de definities van de diverse risico's vast en zal per risico het beleid, de uitvoering van het beleid en de controle toelichten aan de hand van het three lines of defence model. Aan het eind van elk jaar, of indien dit eerder nodig is, zal het beleid worden geëvalueerd en zo nodig aangepast. Zodoende ontstaat een doorlopend governance-proces De eerste beheersingslijn wordt gevormd door het uitvoerend bestuur met ondersteuning van het bestuursbureau, de tweede beheersingslijn wordt gevormd door de Compliance Officer en de Risk Manager en de derde lijn door de internal audit. De taken van de drie beheerslijnen worden hieronder per integriteitsrisico verder toegelicht.

### Toepassingsbereik

Het integriteitsbeleid ziet op de naleving van externe wet- en regelgeving, waarvan de integriteitsrisico's en –thema's worden afgeleid en beschreven. Het pensioenfondsv heeft het toepassingsbereik van de wetgeving voor de specifieke integriteitsrisico's als volgt gedefinieerd:

- Pensioenwet (en lagere regelgeving)
  - Besluit uitvoering pensioenwet en wet verplichte beroepspensioenregeling;
  - Regeling pensioenwet en wet verplichte beroepspensioenregeling;
  - Besluit Financieel Toetsingskader;
  - Code Pensioenfondsv;
- Wet bedrijfstakpensioenfondsv 2000;
  - Vrijstellings- en boetebesluit Wet Bpf 2000
- Beleid van DNB en AFM;
- Sanctiewet- en regelgeving, waaronder bepalingen van:
  - Europese Unie;
  - United Nations;
  - OFAC;
  - Her Majesty's Treasury ("HMT"/United Kingdom);

- Privacy wetgeving, waaronder de Algemene Verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening gegevensbescherming;
- Burgerlijk wetboek (voor zover van toepassing op de integriteitsthema's);
- Wetboek van strafrecht;
- Wet op de economische delicten;
- Internationale wet- en regelgeving (met uitzondering van de hiervoor onder de reikwijdte genoemde wet- en regelgeving);
- Mededingingswet;
- Fiscale wet- en regelgeving.

## Evaluatiedata

Alle integriteitsonderwerpen worden elk jaar in het najaar door het bestuur geëvalueerd. Hieronder zijn de verschillende integriteitsonderwerpen opgenomen.

1. Integriteitsbeleid algemeen
2. Fraude/Corruptie
3. Witwassen
4. Terrorismefinanciering en naleving sanctiewetgeving
5. Belangenverstrengeling /omkoping
6. Handel voorwetenschap
7. Onethisch handelen
8. Fiscaliteit
9. IT
10. Privacy

## Rapportages intern

De compliance officer rapporteert 1 x per jaar schriftelijk aan het bestuur over integriteitsrisico's.

Onderwerp	Uitvoering door
Fraude/Corruptie	Compliance officer
Witwassen <sup>1</sup>	Portefeuillehouders Vermogensbeheer en Risicobeheer
Terrorismefinanciering en naleving sanctiewetgeving <sup>1</sup>	Portefeuillehouders Vermogensbeheer, Risicobeheer en Pensioenregeling en communicatie
Belangenverstrengeling /omkoping	Compliance officer
Handel voorwetenschap	Compliance officer
Onethisch handelen	Compliance officer

<sup>1</sup> Procesafspraken moeten nog gemaakt worden.

Fiscaliteit	Portefeuillehouder Risicobeheer coördineert  Portefeuillehouder Vermogensbeheer: BTW en beleggingen  Portefeuillehouder Pensioenregeling en communicatie: loonbelasting
-------------	--

### Rapportage uitbestedingsrelaties

Het pensioenfonds heeft in Q1 2016 een format opgesteld voor een compliance rapportage. Deze rapportage wordt periodiek (op kwartaalbasis) verstrekt aan de vermogensbeheerders (SAREF, State Street Global AM & SEI) van het pensioenfonds, waarbij de vermogensbeheerders aangeven welke incidenten en ontwikkelingen zich binnen de organisatie hebben voorgedaan op de door het pensioenfonds gedefinieerde onderdelen van het integriteitsbeleid.

Centric rapporteert op kwartaalbasis in een rapportage inzake integriteitsonderwerpen binnen Centric. Deze rapportages worden door het bestuur aan de compliance officer verstrekt ten behoeve van de jaarlijkse rapportage inzake integriteit van de Compliance Officer aan het bestuur.

## 2 Integriteit algemeen

### Inleiding

Het pensioenfonds stimuleert de toegenomen aandacht aan het onderdeel integriteit en de bijbehorende risico's en is actief bezig geweest om stappen te nemen om het volwassenheidsniveau met betrekking tot integriteit voor het pensioenfonds naar een hoger niveau te tillen.

### Integer gedrag

Bij integer gedrag gaat het om een professionele, individuele verantwoordelijkheid waarbij iemand zich bewust is van, en zorgvuldig rekening houdt met rechten, belangen en wensen van belanghebbenden, een open en transparante houding heeft en bereid is om (professionele) verantwoordelijkheid te nemen en verantwoording af te leggen over genomen beslissingen en acties.

### Integere cultuur

Een integere cultuur is de sfeer en het klimaat waarin het pensioenfonds zich ook in ruimere zin gedraagt of handelt op een manier die uitlegbaar en te verantwoorden is waarbij integer gedrag gestimuleerd en beloond wordt en waarbij niet alleen de letter van de wet, maar ook de geest ervan wordt nageleefd.

### Integriteit

Integriteit valt uiteen in vier vormen: **persoonlijke, relationele, organisatorische** en **marktintegriteit**. Onder persoonlijke integriteit valt, maar daartoe niet gelimiteerd betrouwbaarheid, openheid en bewustzijn. Bij relationele integriteit moet men denken aan vragen als wie zijn de stakeholders, welke belangen spelen er en zijn er afhankelijkheden tussen verschillende partijen. Onderwerpen als openheid, organisatiestructuur en verantwoordingscultuur vallen onder organisatorische integriteit. Bij marktintegriteit wordt de vraag gesteld of de betrokkenen bij het pensioenfonds op een terughoudende wijze omgaan met beschikbare marktinformatie en maken zij daar in hun privé-situatie geen misbruik van? Tevens kan de vraag worden gesteld of er pogingen worden gedaan om koersen te manipuleren? Met dit uitgangspunt zijn per integriteitcomponent mogelijke beheersmaatregelen opgenomen ten behoeve van de beheersing van de integriteitsrisico's.

### Integriteitsrisico's

Het pensioenfonds moet zorgdragen voor een systematische analyse van integriteitsrisico's en aan de hand van deze analyse een integriteitbeleid vaststellen. Integriteitsrisico is het risico van sancties en verlies als gevolg van het niet fatsoenlijk handelen of gedragen. Voor het pensioenfonds is de best practice dat cultuur en integriteit aansluit bij de risicomanagementcyclus waarbij een eindverantwoordelijke is benoemd.

Om het integriteitsbeleid vast te stellen moet met een aantal zaken rekening gehouden worden. Het bestuur is eindverantwoordelijk om integriteitsonderwerpen vast te stellen. De volgende elementen zullen hierbij in ieder geval gehanteerd worden:

#### - **Risico-identificatie**

De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse. Hierbij worden de 4 in de inleiding omschreven integriteitsvormen als uitgangspunt genomen. Deze identificatie heeft ultimo 2015 plaatsgevonden.

- **Risicobeleid**  
De kwaliteit van het vastgelegde beleid over de mate waarin en de wijze waarop men de betreffende risicocategorie wenst te beheersen. Deze notitie vormt hier een uitwerking van.
- **Administratieve organisatie en interne controle**  
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd ten einde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.
- **Risicomonitoring**  
De uitkomsten van de systematische analyse integriteitsrisico's worden opgenomen in de tooling die het pensioenfonds hanteert om de risico inschattingen te monitoren, namelijk Risicomaat. Daarnaast beoordeelt de risicocommissie van het pensioenfonds periodiek de ontvangen compliance rapportages van de uitbestedingsrelaties.

De kans en de impact bij het optreden van de geïdentificeerde risico's vormen daarbij een cruciaal onderdeel.

Gewenste beheersingsniveaus –te weten het verminderen van de kans en/of impact van risico's- worden bereikt door middel van (nieuwe) beheersingsmaatregelen. Sommige risico's moeten worden geëlimineerd (grote impact), anderen worden beheerst. Kleine risico's kunnen worden geaccepteerd (lage waarschijnlijkheid / kleine impact). Voor het bestuur is dit een doorlopend proces.

### **Risicoanalyse**

Door periodiek de systematische integriteit risicoanalyse (SIRA) te herhalen en vast te leggen wordt de voortgang in implementatie en naleving zichtbaar. De SIRA wordt elk jaar door de Portefeuillehouders Risicobeheer van het pensioenfonds gecontroleerd om te bekijken of de inschattingen van de risico's nog aansluiten bij het beleid van het pensioenfonds en wat de status is van de gedefinieerde actiepunten uit deze analyse. Als er tussentijds sprake is van 'triggerevents' (bijvoorbeeld als gevolg van wijzigingen in wet- regelgeving, wijzigingen in het beleid en de processen van het pensioenfonds, of incidenten) dan zal de SIRA tussentijds worden gecontroleerd door de Portefeuillehouders Risicobeheer en zal zo nodig een voorstel tot aanpassing worden gedaan.

### **Beleid en Three lines of defence**

In dit integriteitsbeleid zijn de normenkaders, de definitie, het beleid en de uitwerking daarvan aan de hand van het three lines of defence-model vastgesteld per deelonderwerp. Naast de hieronder aangegeven controle die wordt uitgevoerd per risico, wordt door de Compliance Officer elk jaar een workshop gegeven over de risico's die in dit integriteitsbeleid zijn vastgelegd. Daarnaast zijn er meer generieke thema's (governance en HR) die voor de sub risico's van belang zijn. Tevens is het van belang om vast te stellen dat in 2018 de systematische analyse integriteitsrisico's zal worden geactualiseerd. De actiepunten die daaruit naar voren komen zullen in daarna in dit document worden verwerkt.

Het integriteitsbeleid bevat de volgende risico's:

1. Fraude/corruptie
2. Witwassen
3. Terrorismefinanciering en naleving sanctiewetgeving
4. Belangenverstremeling/omkoping
5. Handel voorwetenschap
6. Onethisch handelen
7. Fiscaliteit
8. IT
9. Privacy

Daarnaast hanteert het pensioenfonds ook 2 overkoepelende generieke risico categorieën, namelijk:

1. HR
2. Governance

In de volgende hoofdstukken worden deze onderdelen nader toegelicht. Hierbij noemen we de beheersingsmaatregelen van het pensioenfonds op hoofdlijnen gegeven de diepgang van de systematische analyse van integriteitsrisico's.

### **Algemene Verordening Gegevensbescherming (AVG)**

Het pensioenfonds voert de bedrijfstakpensioenregeling uit. In dit kader verwerkt het pensioenfonds persoonsgegevens. Hierop is de AVG van toepassing. Deze Europese verordening heeft als doel om te borgen dat:

1. noodzakelijke en passende beveiligingsmaatregelen worden getroffen om de persoonsgegevens te beschermen; en
2. betrokkenen hun rechten kunnen uitoefenen voor wat betreft de verwerking van hun persoonsgegevens.

Bij de invulling van het integriteitsbeleid houdt het pensioenfonds hier uitdrukkelijk rekening mee. Het pensioenfonds heeft in dit kader de wijze waarop zij invulling geven aan de naleving van de AVG vastgelegd in een nieuw privacyreglement en de gedragscode. Tevens heeft het bestuur een Functionaris Gegevensbescherming in de zin van de AVG aangesteld.

## **Generieke beheersing: HR**

### **Definitie**

Human resource management betekent letterlijk 'beheer van menselijke productiemiddelen'. Het systematisch managen van personeel in een flexibele, open keten met oog voor transparantie, communicatie, samenwerking en veranderingen, op zodanig motiverende en op het fonds afgestemde wijze, dat het personeel zo veel mogelijk toegerust wordt met bagage waarmee zij hun werk vorm en inhoud kunnen geven. Onderdelen van Human Resources ziet het pensioenfonds als een overkoepelend integriteitsrisico. Immers indien deze onderdelen niet goed zijn ingeregeld, kan dit effect hebben op alle specifieke integriteitsrisico's.

Onderdelen hiervan zijn:

- Recrutment
- Beloning

### **Beleid**

Het pensioenfonds kent een selectieprocedure voor nieuwe bestuursleden inclusief interviews en assessment. Daarnaast worden nieuwe bestuursleden van het pensioenfonds getoetst bij en gescreend door DNB. Disciplinaire maatregelen zoals ontslag zijn opgenomen in de contracten met de uitvoerende bestuursleden alsmede in de statuten van het pensioenfonds. Het pensioenfonds kent een beheerst beloningsbeleid. Daarnaast worden betalingen aan bestuursleden altijd behandeld middels een vierogen principe.

In de protocollen uitbestedingsbeleid en adviesrelaties is opgenomen dat deze externe dienstverleners een aanvaardbaar beloningsbeleid dienen te voeren. Het beloningsbeleid maakt onderdeel uit van de contractafspraken. In de jaarlijkse evaluatie van de externe dienstverleners wordt het beloningsbeleid eveneens meegenomen. In het protocol uitbestedingsbeleid en adviesrelaties is vastgelegd dat de uitbestedings- en adviesrelatie over een integriteitsbeleid en HRM beleid beschikt.



## **Three lines of defence**

### **Eerste lijn**

De uitvoerende bestuursleden zijn verantwoordelijk voor het opstellen en uitvoeren van het beleid ten aanzien van recruitment en beloning dat hiervoor is genoemd. De niet uitvoerende bestuursleden zien daarop toe en controleren de uitvoering van het beleid van het bestuur. Daarnaast staat het de uitvoerende bestuurders met raad ter zijde.

Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken.

### **Tweede lijn**

Het pensioenfonds heeft een Compliance Officer die toezicht houdt op de deugdelijkheid en effectiviteit van interne regels en procedures. Daarnaast adviseert en informeert de Compliance Officer verbonden personen gevraagd en ongevraagd over de uitleg en toepassing van de gedragscode. Binnen het pensioenfonds vindt er sociale controle plaats.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake integriteit, waaronder HR. Als de Compliance Officer constateert dat het pensioenfonds buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van HR.

### **Derde lijn**

De internal audit voert periodiek audits uit om de te beoordelen of de eerste lijn en tweede lijn hun verantwoordelijkheden zijn nagekomen ten aanzien van deze recruitment en belonings-processen.

## **Generieke beheersing: governance**

### **Definitie**

Het doel van governance is het scheppen van waarborgen voor realisatie van die doelstellingen. Het fonds dient daartoe gestuurd en beheerst te worden en over die activiteiten dient verantwoording aan de belanghebbenden te worden afgelegd, in veel gevallen via een formele of informele toezichthouder die namens die belanghebbenden opereert. Daarmee omvat governance de activiteiten van sturen, beheersen, toezicht houden en verantwoorden, hetgeen waarvoor het uitvoerend bestuur in eerste aanleg verantwoordelijk is. Onderdelen van governance ziet het pensioenfonds als een overkoepelend integriteitsrisico. Immers indien deze onderdelen niet goed zijn ingeregeld, heeft dit effect op alle specifieke integriteitsrisico's.

Onderdelen hiervan zijn:

- Structuur, beleid en procedures
- Cultuur

## **Beleid**

Het pensioenfonds hanteert een duidelijke governance structuur aan de hand van het three lines of defence model waarin helder is wat duidelijke rollen en verantwoordelijkheden per orgaan en per bestuurslid zijn. Daarmee wordt voorkomen dat opzet, het bestaan en de werking van beleid, de uitvoering ervan en de toetsing ervan in dezelfde beheerslijn plaatsvindt. Een duidelijke governance structuur is een voorwaarde om een degelijk riskmanagement framework te kunnen inrichten.

Het bestuur heeft de rollen en verantwoordelijkheden met betrekking tot het Integraal Risicomanagement van het bestuur, het bestuursbureau, de portefeuillehouders, de Compliance Officer, de Risk Manager en de Internal audit geëvalueerd aan de hand van een RACI tabel.

In het geschiktheidsplan zijn cultuur aspecten benoemd.

## **Three lines of defence model**

### **Eerste lijn**

Het bestuur van het pensioenfonds hecht belang aan zijn eigen gedrag, hun samenwerking, leiderschap en besluitvormingswijze te reflecteren. Het bestuur evalueert, het eigen gedrag en de groepsdynamiek binnen het bestuur en reflecteert op zaken als interne en externe samenwerking, de manier waarop besluiten worden genomen, het voorzitterschap e.d. Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken. Jaarlijks wordt samen met de Compliance Officer een keuze gemaakt om thema's uit de generieke beheersing in een workshop te behandelen. De verantwoordelijkheid voor de handhaving van de governance ligt bij het uitvoerend bestuur met ondersteuning van medewerkers van het bestuursbureau. Zij dienen het geformuleerde governance beleid uit te voeren, en zorg te dragen voor het implementeren en onderhouden van voldoende beheersingsmaatregelen voor een goede uitvoering. Het bestuur is verantwoordelijk voor het compliant zijn en blijven van het pensioenfonds. Daarbij houdt het niet-uitvoerend bestuur toezicht en is daarmee afgeleid verantwoordelijk voor het beheersen van de governance van het pensioenfonds.

### **Tweede lijn**

De tweede lijn in het model bestaat uit de Compliance Officer en de risk manager en bewaakt de uitoefening van het beleid van het bestuur aan de hand van het controleren van de risicobeheersing in de operationele werkzaamheden en processen in de eerste lijn. De Compliance Officer biedt hierbij ondersteuning en adviseert over het uit te voeren beleid waarbij vervolgens wordt gerapporteerd aan het bestuur. De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake integriteit. Als de Compliance Officer constateert dat het pensioenfonds buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen.

Door de tweede lijn wordt op kwartaalbasis aan de Auditcommissie gerapporteerd. Verder heeft de tweede lijn een onafhankelijke escalatielijn richting de voorzitter van het bestuur.

### **Derde lijn**

De derde beheersingslijn wordt gevormd door internal audit welke als primaire taak heeft het controleren of de eerste en tweede beheersingslijn hun verantwoordelijkheden zijn nagekomen. Voor de structuur van het pensioenfonds is het van belang dat deze derde lijn extern wordt ingehuurd. Internal Audit is onafhankelijk gepositioneerd ten opzichte van het uitvoerend bestuur en rapporteert vanuit deze positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van de governance zijn nagekomen.

### 3 Integriteitsthema's

#### Fraude/ corruptie

##### Definitie

Fraude is een vorm van bedrog; de zaken worden anders voorgesteld dan ze zijn, door op papier of digitaal een onjuiste weergave te geven van de werkelijkheid. Het wetboek van strafrecht kent een aantal artikelen dat op allerlei vormen van bedrog betrekking heeft. Eén ervan is het misdrijf oplichting, dat het meest algemeen van karakter is en (enigszins verkort) als volgt wordt omschreven: "Met het oogmerk om zichzelf of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iets of iemand bewegen tot de afgifte van een (financieel) goed, tot het ter beschikking stellen van. Bij Corruptie verleent iemand in een machtspositie ongeoorloofde gunsten in ruil voor wederdiensten of als vriendendienst.

##### Beleid

Het pensioenfonds heeft een gedragscode en een klokkenluiders- en incidentenregeling. De klokkenluiders- en incidentenregeling bepaalt dat een melding van een incident of een misstand bij de Compliance Officer wordt gedaan. De Compliance Officer informeert de voorzitter hierover en stelt vervolgens een onderzoek in.

##### Three lines of defence

###### Eerste lijn

De uitvoerende bestuursleden zijn verantwoordelijk voor de beleidsvoorbereiding en dragen zorg voor de uitvoering van het beleid ten aanzien van het voorkomen van fraude en corruptie. De uitvoerende bestuursleden leggen verantwoording af aan de niet-uitvoerende bestuurders ten aanzien van het beleid over fraude en corruptie. De niet-uitvoerende bestuursleden (met portefeuille Governance en Compliance) houden toezicht en zien toe op de uitvoering van het beleid van het uitvoerend bestuur ten aanzien van fraude en corruptie en staan het uitvoerend beleid met raad terzijde. Ten aanzien van de uitbestedingspartners is in het uitbestedingsbeleid vastgelegd dat het bestuur en haar zakelijke relaties zijn gehouden aan de vigerende wet- en regelgeving en het bestuur zorgt ervoor dat de gedragscode van de uitbestedingspartner minimaal gelijkwaardig is aan de gedragscode van het pensioenfonds. Verder heeft het fonds een tweehandtekeningclausule. Dit betekent dat de onafhankelijke voorzitter en een uitvoerend bestuurslid gezamenlijk documenten moeten ondertekenen waardoor de mogelijkheid op fraude wordt beperkt

###### Tweede lijn

De Compliance Officer rapporteert elk jaar aan het bestuur of hij meldingen heeft ontvangen over incidenten en/of misstanden en de aard daarvan. Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken. Ten aanzien van de uitbesteding wordt jaarlijks de SLA getoetst aan het uitbestedingsbeleid en de relevante wet- en regelgeving. De Compliance Officer ziet toe op de melding van de mogelijke incidenten en misstanden welke jaarlijks worden gerapporteerd aan het bestuur.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake fraude en corruptie. Als de Compliance Officer constateert dat het pensioenfonds voor deze risico's buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer

en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van fraude en corruptie.

### **Derde lijn**

De Internal Audit bewaakt de uitvoering en de processen van de eerste en tweede lijn ten aanzien van het voorkomen van fraude en corruptie. De Internal Audit ontvangt opdrachten van het niet-uitvoerend bestuur. Het uitvoerend bestuur, de compliance officer en de risk manager kunnen daarnaast het niet-uitvoerend bestuur verzoeken bepaalde onderwerpen inzake fraude op de auditagenda te plaatsen.

## **Witwassen**

### **Definitie**

Het risico dat schade ontstaat met betrekking tot de reputatie, financiële schade en/of schade door preventief dan wel repressief optreden door de bevoegde autoriteiten als gevolg van (ongewilde) betrokkenheid bij witwassen door klanten, tussenpersonen dan wel eigen personeel. Specifiek van belang: Wet ter voorkoming van witwassen en financieren van terrorisme.

### **Beleid**

Het pensioenfonds maakt gebruik van een implicatieprocedure. Dit betekent dat bij ieder beleidsvoorstel een risicoparagraaf wordt toegevoegd om de risico's inzichtelijk te maken. Verder waarborgt het uitbestedingsbeleid dat het selecteren en de uitvoering van partijen waaraan wordt uitbesteed, zoals de externe vermogensbeheerder en pensioenadministrateur, op een zorgvuldige manier gebeurt. Het uitvoerend bestuur heeft (conform de bestaande protocollen) contractueel met haar zakelijke relaties vastgelegd dat het bestuur en haar zakelijke relaties zijn gehouden aan de vigerende wet- en regelgeving.

### **Three lines of defence**

#### **Eerste lijn**

De uitvoerende bestuursleden zijn verantwoordelijk voor de beleidsvoorbereiding en dragen zorg voor de uitvoering van het beleid ten aanzien van het voorkomen van witwassen. De uitvoerende bestuursleden leggen verantwoording af aan de niet-uitvoerende bestuurders ten aanzien van het beleid over witwassen. De niet-uitvoerende bestuursleden (met portefeuille Governance en Compliance) houden toezicht en zien toe op de uitvoering van het beleid van het uitvoerend bestuur over het voorkomen van witwassen en staan het uitvoerend beleid met raad terzijde. Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken. De SLA, die is overeengekomen met de uitbestedingspartners, wordt periodiek getoetst, conform het uitbestedingsbeleid.

#### **Tweede lijn**

De Compliance Officer draagt de zorg over de uitvoering en vastleggen van incidenten inzake witwassen. Jaarlijks rapporteert de Compliance Officer de meldingen aan het bestuur. De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake witwassen. Als de Compliance Officer constateert dat het pensioenfonds voor deze risico's buiten of op de rand van de risk-appetite van het

pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van witwassen.

### **Derde lijn**

Internal Audit rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van incidenten inzake witwassen zijn nagekomen aan de hand van periodieke audits.

## **Terrorismefinanciering en naleving sanctiewetgeving**

### **Definitie**

Het risico dat de reputatie (van het pensioenfonds en de toezichthouder) wordt beïnvloed als gevolg van het verrichten van handelingen door het pensioenfonds met natuurlijke en/of rechtspersonen die betrokken zijn bij het (financieren van) terrorisme of criminaliteit op basis van specifieke wetgeving.

### **Beleid**

DNB publiceert jaarlijks een lijst van personen en organisaties die in verband gebracht worden met terroristische activiteiten. De klokkenluiders- en incidentenregeling van het pensioenfonds bepaalt dat een strafbaar feit (aldus terrorismefinanciering en sanctiewetgeving) aangemerkt wordt als een incident. De uitbestedingspartners screenen regelmatig aan de hand van de gepubliceerde lijsten hun administratie. Daarnaast sluit het beleggingsplan van het pensioenfonds bedrijven die zich bezighouden met controversiële wapens uit.

In de ISAE verklaring wordt gerapporteerd worden over de controle op dit onderwerp.

### **Three lines of defence**

#### **Eerste lijn**

Het bestuur heeft (conform de bestaande protocollen) contractueel met haar zakelijke relaties vastgelegd dat het bestuur en haar zakelijke relaties zijn gehouden aan de vigerende wet- en regelgeving ten aanzien van terrorismefinanciering en naleving van de sanctiewetgeving. De uitvoerende bestuursleden zijn verantwoordelijk voor de beleidsvoorbereiding en dragen zorg voor de uitvoering van dit beleid. De niet-uitvoerende bestuursleden (met portefeuille Governance en Compliance) houden toezicht, zien toe op de uitvoering van dit beleid van het bestuur en staan het uitvoerend beleid met raad terzijde.

#### **Tweede lijn**

Overtreding van de regels ten aanzien van terrorismefinanciering en naleving van de sanctiewetgeving levert een incident op. Volgens de Klokkenluiders- en incidentenregeling moet een incident gemeld worden aan de Compliance Officer. De Compliance Officer informeert de voorzitter hierover en stelt vervolgens een onderzoek in. Daarnaast rapporteert de Compliance Officer elk jaar aan het uitvoerende bestuur over de gemelde incidenten.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake terrorismefinanciering en naleving van de sanctiewetgeving. Als de Compliance Officer constateert dat het pensioenfonds voor deze risico's buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken

aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van terrorismefinanciering en naleving van de sanctiewetgeving.

### **Derde lijn**

De Interne Audit voert periodiek audits uit met betrekking tot deze onderwerpen en rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van het beleid met betrekking tot terrorismefinanciering en naleving van de sanctiewetgeving zijn nagekomen.

## **Belangenverstreming/ omkoping**

### **Definitie**

Belangenverstreming omvat de situatie waarbij een betrokkene meerdere belangen dient, die een zodanige invloed op elkaar kunnen uitoefenen dat de integriteit ten aanzien van het ene belang of het andere belang in het geding komt.

Pensioenfondsen dienen te voorkomen dat bestuurders (waaronder ook het orgaan dat belast is met toezicht op het beleid en de algemene gang van zaken), medewerkers en personen die in opdracht van het fonds werkzaamheden verrichten betrokken raken bij belangenconflicten en tevens dat deze personen geen misbruik en oneigenlijk gebruik maken van informatie of zaken die aanwezig zijn bij het fonds, waardoor de stabiliteit en de integriteit van de financiële markten gewaarborgd blijft.

Omkoping is het risico dat bestuurders of medewerkers van het pensioenfonds worden omgekocht of anderen omkopen

### **Beleid**

De gedragscode draagt mede bij aan het integer functioneren van het pensioenfonds ten behoeve van al diegenen die bij het pensioenfonds belang hebben en het waarborgen van de goede naam en reputatie van het pensioenfonds en de pensioensector in het algemeen. Daarvoor dient elke potentieel belangenconflict en dus belangenverstreming vermeden te worden en direct gemeld te worden aan de Compliance Officer. Daarnaast dienen de uitbestedingspartners van het pensioenfonds te beschikken over een gedragscode die voldoet aan wet- en regelgeving en minimaal gelijkwaardig is aan die van het pensioenfonds.

Omkoping kan tot onzuivere besluitvorming leiden en hierdoor kan het pensioenfonds schade oplopen in financiële zin dan wel in de zin van reputatie.

De risico analyse inzake omkoping is in eerste instantie gebaseerd op de gedragscode waarin specifiek is uitgewerkt hoe met bovengenoemde situaties moet worden omgegaan en kunnen er aanvullend andere gedragsregels voor de betrokkenen gelden. Deze aanvullende gedragsregels zullen indien relevant voor de specifieke situatie worden opgesteld. Daarnaast geldt een uitbestedingsbeleid.

Het beleid zal via de gebruikelijke interne communicatiemiddelen gecommuniceerd worden, zodat dit voor alle betrokkenen bekend is. Zowel vanaf het begin van de betrokkenheid van personen als bij iedere update van het beleid. Tevens zal het beleid intern bereikbaar zijn voor alle betrokkenen.

## **Three lines of defence**

### **Eerste lijn**

De uitvoerende bestuursleden zijn verantwoordelijk voor de beleidsvoorbereiding en dragen zorg voor de uitvoering van het beleid ten aanzien van belangenverstreming en omkoping. De niet uitvoerende bestuursleden (met portefeuille Governance en Compliance) houden toezicht op dit beleid en staan het

uitvoerend beleid met raad terzijde. De niet-uitvoerende bestuursleden nemen bij de uitvoering van hun taken te allen tijde de Gedragscode en Code pensioenfondsen in acht.

Daarnaast houdt het pensioenfonds jaarlijks een integrale risicoanalyse waarin deze integriteitsrisico's worden meegenomen en besproken.

### **Tweede lijn**

Elk potentieel belangenconflict en dus belangenverstremgeling dient vermeden te worden en direct gemeld te worden aan de Compliance Officer. De verbonden personen maken in de kwartaal uitvraag naleving gedragscode melding van onderwerpen die kunnen leiden tot reputatieschade of belangenconflict. Voorbeelden van deze onderwerpen zijn beïnvloeding door relatiegeschenken en uitnodigingen en nevenfuncties, financiële belangen, privégebruik fondsleveranciers, gebruik pensioenfondseigendommen, voorwetenschap en privé transacties door insiders. De Compliance Officer rapporteert elk kwartaal over het onderzoek dat hij uitvoert ten aanzien van de meldingen die worden gedaan door de verbonden personen.. De compliance Officer rapporteert aan het bestuur en staat het bestuur met raad ter zijde.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake belangenverstremgeling en omkoping. Als de Compliance Officer constateert dat het pensioenfonds voor deze risico's buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van belangenverstremgeling en omkoping.

### **Derde lijn**

De Internal Audit voert periodiek audits uit en rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van het beleid inzake belangenverstremgeling en omkoping zijn nagekomen.

## **Handel voorwetenschap**

### **Definitie**

Het risico voor het pensioenfonds dat door (werknemers dan wel de leiding van) het pensioenfonds misbruik wordt gemaakt van voorkennis over ontwikkelingen dan wel rechtspersonen. Onder misbruik vallen ook effectentransacties waarbij gebruik wordt gemaakt van verkregen voorkennis. Zie de Gedragscode.

### **Beleid**

Het pensioenfonds beschikt over een gedragscode. In deze gedragscode is vastgelegd dat verbonden personen geen gebruik mogen maken van voorwetenschap. Verbonden personen dienen bij aanvang van hun functie een aanvangsverklaring te ondertekenen waardoor zij aangeven op de hoogte te zijn van (onder andere) deze bepaling.. Verder heeft het pensioenfonds een insidersregeling.

## **Three lines of defence**

### **Eerste lijn**

De uitvoerende bestuursleden zijn verantwoordelijk voor de beleidsvoorbereiding en dragen zorg voor de uitvoering van het beleid ten aanzien van het voorkomen van handelen met voorwetenschap. De niet-uitvoerende bestuursleden (met portefeuille Governance en Compliance) houden toezicht op dit beleid en staan het uitvoerend beleid met raad terzijde. Het pensioenfonds houdt daarnaast jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken. Het uitvoerend bestuur legt vervolgens verantwoording af aan de niet-uitvoerende bestuursleden ten aanzien van het beleid.

### **Tweede lijn**

De Compliance Officer toetst de naleving van de gedragscode van het pensioenfonds, waar de insiderregeling een onderdeel van is. Ieder kwartaal dienen de verbonden personen en insiders een verklaring naleving gedragscode in te vullen en naar de Compliance Officer te sturen, waarin wordt aangegeven door de verbonden personen of er sprake is geweest van voorwetenschap. Tevens dienen bepaalde persoonlijke transacties van insiders gemeld te worden aan de Compliance Officer. Elk kwartaal onderzoekt de Compliance Officer of de door de insiders gemelde persoonlijke transacties samenvallen met de transacties van het pensioenfonds en daardoor enige vorm van voorwetenschap impliceren. De Compliance Officer rapporteert per kwartaal over zijn bevindingen aan het bestuur.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake handel met voorwetenschap. Als de Compliance Officer constateert dat het pensioenfonds voor dit risico buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van handel met voorwetenschap.

### **Derde lijn**

De Internal Audit voert periodiek audits uit en rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van het beleid inzake voorwetenschap zijn nagekomen.

## **Onethisch handelen**

### **Definitie**

Het risico dat de reputatie (en mogelijk ook de financiële positie) van het pensioenfonds wordt beïnvloed als gevolg van het door het pensioenfonds bewust of onbewust faciliteren van, of betrokkenheid hebben bij, overtredingen.

### **Beleid**

De gedragscode zorgt onder andere voor het behoud van de goede naam en reputatie van het pensioenfonds. Daarom dient de gedragscode te worden nageleefd door de verbonden personen. Het handelen door de verbonden persoon in strijd met de gedragscode wordt beschouwd als een ernstige inbreuk op het vertrouwen dat het pensioenfonds in de verbonden persoon moet kunnen stellen. Een dergelijk handelen kan reden zijn tot het opleggen van een sanctie, afhankelijk van de ernst van de overtreding. Daarnaast beschikt het pensioenfonds over een klokkenluiders- en incidentenregeling.



## **Three lines of defence**

### **Eerste lijn**

Het niet-uitvoerend bestuur ziet toe op de uitoefening van het beleid ten aanzien van onethisch handelen. Het uitvoerend bestuur is uiteindelijk verantwoordelijk voor het beleid en past dit indien nodig jaarlijks aan. Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken.

### **Tweede lijn**

De Compliance Officer toetst de naleving van de gedragscode. Naleving van de gedragscode is een van de beheersmaatregelen om onethisch handelen te voorkomen. Volgens de klokkenluiders- en incidentenregeling kunnen incidenten en misstanden gemeld worden aan de Compliance Officer die vervolgens een onderzoek instelt. Onethisch handelen dat kwalificeert als een incident of een misstand wordt op deze wijze beoordeeld door de compliance officer (bij incidenten) of het orgaan waar zich de misstand heeft voorgedaan (bij misstanden). De Compliance Officer van het pensioenfonds is de vertrouwenspersoon voor het bestuur en legt verantwoording af aan het uit te voeren beleid. De Compliance Officer rapporteert elk jaar aan het bestuur over gemelde incidenten en misstanden. De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake onethisch handelen. Als de Compliance Officer constateert dat het pensioenfonds voor dit risico buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van onethisch handelen.

### **Derde lijn**

De Internal Audit voert periodiek audits uit en rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van het beleid inzake onethisch handelen zijn nagekomen.

## **Fiscaliteit**

### **Definitie**

Het risico dat het pensioenfonds meewerkt aan het oneigenlijk gebruik van fiscaal voordelige structuren.

### **Beleid**

Het pensioenfonds heeft een fiscaal adviseur aangesteld voor de BTW. Daarnaast wordt het pensioenfonds op de hoogte gehouden door externe partijen op het gebied van fiscale wetgeving. De agendacommissie van het pensioenfonds is verantwoordelijk voor toezicht op de beheersing en controle van wet- en regelgeving. Tevens zijn de portefeuillehouders Risicobeheer, Vermogensbeheer en Pensioenregeling en communicatie verantwoordelijk voor deelgebieden (BTW en beleggingen versus loonbelasting). Daarnaast wordt er een accountantscontrole uitgevoerd bij de uitbestedingspartners. Verder kunnen fiscale integriteitsrisico's een incident of misstand zijn in de zin van de klokkenluiders- en incidentenregeling van het pensioenfonds.

## **Three lines of defence**

### **Eerste lijn**

Het niet-uitvoerend bestuur ziet toe op de uitoefening van het beleid. Het uitvoerend bestuur is uiteindelijk verantwoordelijk voor het beleid en past dit indien nodig jaarlijks aan. Het pensioenfonds houdt jaarlijks een integrale risicoanalyse waarin dit integriteitsrisico wordt meegenomen en besproken.

### **Tweede lijn**

Volgens de klokkenluiders- en incidentenregeling kunnen incidenten en misstanden gemeld worden aan de Compliance Officer die vervolgens een onderzoek instelt. Fiscale integriteitsrisico's die kwalificeren als een incident of een misstand worden op deze wijze beoordeeld door de compliance officer (bij incidenten) of het orgaan waar zich de misstand heeft voorgedaan (bij misstanden). De Compliance Officer van het pensioenfonds is de vertrouwenspersoon voor het bestuur en legt verantwoording af aan het uit te voeren beleid. De Compliance Officer rapporteert elk jaar aan het bestuur over gemelde incidenten en misstanden.

De rol van de risk manager is het begeleiden en adviseren op risico-assessments inzake fiscale integriteitsrisico's. Als de Compliance Officer constateert dat het pensioenfonds voor dit risico buiten of op de rand van de risk-appetite van het pensioenfonds komt, dan zal de Compliance Officer hierover afstemming hebben met de risk manager. Er vindt ook afstemming plaats tussen de Compliance Officer en de risk officer over eventueel te maken aanpassingen in het beleid en/of de beheersmaatregelen ten aanzien van fiscale integriteitsrisico's.

### **Derde lijn**

De Internal Audit voert periodiek audits uit en rapporteert vanuit zijn positie onafhankelijk over de wijze waarop de eerste en tweede beheersingslijnen hun verantwoordelijkheden ten aanzien van het beleid inzake fiscale integriteitsrisico's zijn nagekomen

## **IT**

De analyse van de IT risico's is vastgelegd in een separaat document. Voor de analyse van deze risico's voor wat betreft integriteit wordt verwezen naar het IT Beleidsdocument.

## **Privacy**

De analyse van de privacy risico's is vastgelegd in een separaat document. Voor de analyse van deze risico's voor wat betreft integriteit wordt verwezen naar het IT Beleidsdocument.

Vastgesteld door het bestuur op 13 juni 2018.