

Handboek Compliance

Stichting Pensioenfonds Thales Nederland

Versie 6 december 2024

Inhoudsopgave

<i>Management Summary</i>	3
1. Inleiding	3
2. Definitie van compliance	4
3. Doelstelling compliance	4
4. Scope en reikwijdte compliance	4
5. De compliance verantwoordelijkheid van het bestuur	5
6. Compliance officer	7
7. Uitbesteding	9
8. Vaststelling	9

Bijlage 1 Integriteitsbeleid

Bijlage 2 Gedragscode Pensioenfonds Thales Nederland

Bijlage 3 Incidentenregeling Stichting Pensioenfonds Thales Nederland

Bijlage 4 Klokkenluidersregeling Stichting Pensioenfonds Thales Nederland

Bijlage 5 Regeling vergoedingen organen van Stichting Pensioenfonds Thales Nederland (SPTN)

Bijlage 6 Compliance rapportage

Management Summary

Het pensioenfonds heeft de definitie, doelstellingen, scope en taken en verantwoordelijkheden van de betrokkenen in het kader van het in stand houden van een integere organisatie, bedrijfsvoering en compliance vastgelegd in het handboek Compliance. Het document belicht het belang dat SPTN hecht aan de inrichting en inbedding van compliance en sluit aan bij de kernwaarden van SPTN. Het wettelijk kader van compliance is opgenomen in o.a. de Pensioenwet en in de Code Pensioenfonds. Er is door het bestuur een compliance officer aangesteld, van wie de taken en bevoegdheden zijn beschreven in het handboek. De compliance officer rapporteert jaarlijks aan het dagelijks bestuur. Het handboek bevat tevens het Integriteitsbeleid, de Gedragscode, de Incidenten- en de Klokkenluidersregeling. Daarnaast is ook de Regeling vergoedingen organen van Stichting Pensioenfonds Thales Nederland (SPTN) opgenomen. Periodiek (minimaal eens in de twee jaar) wordt getoetst of het handboek aanpassing behoeft.

1. Inleiding

Stichting Pensioenfonds Thales Nederland (SPTN) hecht veel waarde aan vertrouwen van de deelnemers. Om dit te bewerkstelligen is het voeren van een integere bedrijfsvoering een belangrijke voorwaarde. Het voeren van een integere bedrijfsvoering gaat verder dan het alleen voldoen aan wet- en regelgeving. Het gaat om het hebben van een cultuur waar het als vanzelfsprekend is dat Pensioenfonds Thales Nederland en de daaraan verbonden personen handelen in overeenstemming met de geldende maatschappelijke normen en de (ongeschreven) wet- en regelgeving. De interne regelgeving en de externe wet- en regelgeving zijn uitsluitend van toepassing op de verbonden personen waaronder de bestuursleden, de medewerkers van het pensioenbureau, leden van de Raad van Toezicht, het Verantwoordingsorgaan en externe leden van commissies. Het Pensioenfonds heeft de pensioenadministratie en het vermogensbeheer geheel uitbesteed. Het bestuur stelt tevens eisen aan het gedrag dat medewerkers van externe partijen (daaronder begrepen de vermogensbeheerder, pensioenadministrateur en de custodian) vertonen. Het bestuur verwacht dat de medewerkers van deze partijen voldoen aan interne regelgeving en externe wet- en regelgeving en beschikken over een gedragsregeling die minimaal gelijkwaardig is aan die van SPTN.

Het bestuur is en blijft eindverantwoordelijk voor een integere bedrijfsvoering. De compliance officer ondersteunt het bestuur bij de invulling van deze verantwoordelijkheid. Dit handboek bevat de uitgangspunten van compliance en integriteit door de definitie, doelstellingen, scope en taken en verantwoordelijkheden van de betrokkenen in het kader van het in standhouden van een integere organisatie, bedrijfsvoering en compliance binnen Pensioenfonds Thales te benoemen.

2. Definitie van compliance

De missie van Stichting Pensioenfonds Thales Nederland (SPTN) is als volgt samen te vatten: SPTN voert als zelfstandig pensioenfonds de pensioenregeling uit die tussen de sociale partners is overeengekomen. Dat doen we op een economisch verantwoorde en transparante manier. We zetten het belang van onze (gewezen) deelnemers en pensioengerechtigden voorop en houden ze zo duidelijk en volledig mogelijk op de hoogte van ontwikkelingen rond hun pensioen.

Voor het behalen van deze missie is een integere bedrijfsvoering en de naleving van wet- en regelgeving een noodzakelijke voorwaarde.

SPTN definieert compliance als “het geheel van maatregelen dat zich richt op de implementatie, handhaving en naleving van externe wet- en regelgeving, alsmede op interne regelgeving om te voorkomen dat de reputatie en integriteit van het pensioenfonds wordt aangetast”.

3. Doelstelling compliance

Doelstelling van compliance is het bevorderen van integer gedrag. Een cultuur waarbij het als vanzelfsprekend is dat SPTN en de daaraan verbonden personen handelen in overeenstemming met de geldende maatschappelijke normen en de (ongeschreven) wet- en regelgeving. Een cultuur waarin de professionele, individuele verantwoordelijkheid gestimuleerd en beloond wordt.

4. Scope en reikwijdte compliance

De compliancefunctie ziet toe op de naleving van interne en externe wet- en regelgeving *voor zover deze betrekking heeft op compliance & integriteit en toezicht regelgeving*. De interne complianceregels en -procedures zijn hiervan afgeleid en beschreven.

Het fonds heeft de reikwijdte van de compliancefunctie als volgt gedefinieerd:

- Wet financieel toezicht (Wft);
- Besluit financieel toetsingskader pensioenfonds;
- Besluit Marktmisbruik Wft;
- Code Pensioenfonds;
- Sanctiewet 1977 en onderliggende regelingen;
- Algemene verordening gegevensbescherming (AVG);
- Uitvoeringswet (AVG);
- Pensioenwet (inclusief Pension Fund Governance en lagere regelgeving);
- Besluit uitvoering pensioenwet en wet verplichte beroepspensioenregeling;
- Regeling pensioenwet en wet verplichte beroepspensioenregeling;
- Beleidsregels toezichthouders;
- Beleidsregels, leidraden en good practices van DNB en AFM;
- Burgerlijk wetboek (voor zover van toepassing op de compliance thema's).

De gedragscode van het fonds is een uitwerking van de gedragscode als genoemd in het Besluit Financieel Toetsingskader Pensioenfondsen en het Besluit Marktmisbruik financiële ondernemingen Wft. In de gedragscode zijn eveneens bepalingen opgenomen die voortvloeien uit de Wet op het financieel toezicht.

Daarnaast heeft het fonds interne regelingen ingevoerd, waaronder:

- Integriteitsbeleid
- Uitbestedingsbeleid
- Incidenten-en klokkenluidersregeling
- Beloningsbeleid

Onderstaande wet- en regelgeving valt buiten de reikwijdte van de compliancefunctie:

- Wetboek van strafrecht;
- Wet op de economische delicten;
- Burgerlijk wetboek (voor zover niet van toepassing op de compliance thema's);
- Internationale wet- en regelgeving (met uitzondering van de hiervoor onder de reikwijdte genoemde wet- en regelgeving);
- Mededingingswet;
- Fiscale wet- en regelgeving.

5. De compliance verantwoordelijkheid van het bestuur

Het bestuur van SPTN is en blijft eindverantwoordelijk voor het compliant zijn van SPTN, ook wanneer de uitvoering van de pensioenadministratie en het vermogensbeheer is uitbesteed. Het bestuur van SPTN is daarmee verantwoordelijk voor het inrichten en in stand houden van een effectieve compliance functie.

De taken en verantwoordelijkheden van het bestuur van het fonds aangaande compliance betreffen onder meer:

a. het waarborgen van de integriteit en betrouwbaarheid van het fonds door middel van implementatie van alle verplichtingen uit hoofde van externe wet- en regelgeving en het opstellen van de daarvan afgeleide interne regels en procedures.

Dat betekent dat op verschillende gebieden een aantal waarborgen door het bestuur zijn ingebouwd:

- het inregelen van 'goed bestuur': het beschikken over voldoende deskundigheid door bestuursleden (aantoonbaar);
- screeningsbeleid: (nieuwe) medewerkers worden getoetst op criteria als eerlijkheid, onafhankelijkheid, loyaliteit en integriteit. Door de AIVD wordt een verklaring van geen bezwaar afgegeven (VGB);

- het implementeren van de gedragscode (Modelgedragscode): alle verbonden personen moeten doordrongen zijn van het belang van een goede naleving van de gedragscode;
- het borgen van de complianceaspecten van uitbestede activiteiten door heldere afspraken ten aanzien van compliance te maken met contractpartijen;
- het opstellen van beleid en procedures over de communicatie aan deelnemers (het inbouwen van kwaliteitswaarborgen).

De financiële gegevens van het Pensioenfonds worden jaarlijks gecontroleerd door de accountant en de actuariële grondslagen worden beoordeeld door de waarmerkend actuaaris.

Verder zijn er rapportageverplichtingen en wordt er toezicht gehouden op het Pensioenfonds door DNB en AFM.

Het Pensioenfonds heeft dispensatie op regelniveau van PME (bedrijfstakpensioenfonds Metalektro). Dit punt wordt periodiek getoetst. Het bestuur dient alles in het werk te stellen om aan de transparantie- en informatieverplichtingen tegenover de deelnemers te voldoen.

b. het bevorderen van het compliance- en integriteitsbewustzijn
bij alle verbonden personen, waaronder maar niet beperkt tot het uitdragen van een juiste tone at the top door goed voorbeeldgedrag.

De voorzitter van het bestuur zorgt voor een periodieke agendering, minstens 1 keer per jaar, van compliance/ integriteit in de bestuursvergadering. De manager van het pensioenbureau bespreekt het periodiek, minstens 1 keer per jaar, met de medewerkers van het pensioenbureau.

c. het periodiek afleggen van verantwoording aan de raad van toezicht en verantwoordingsorgaan van het fonds.

Beheerst beloningsbeleid

De bestuursleden en leden van het Verantwoordingsorgaan zijn onbezoldigd. De verbonden personen van het pensioenbureau worden beloond conform de cao Metalektro c.q. Thales NL-arbeidsvoorwaarden waarbij er controle is door de onderneming op een beloning die marktconform is. Leden van de Raad van Toezicht of (externe) adviseurs ontvangen een vergoeding die marktconform is. De Regeling vergoedingen organen van Stichting Pensioenfonds Thales Nederland (SPTN) is opgenomen in bijlage 5.

Teneinde een effectieve compliance functie te bewerkstelligen is de steun van het bestuur en een algemeen gedragen integere bedrijfscultuur onontbeerlijk.

6. Compliance officer

De compliance officer vervult een onafhankelijke rol binnen het pensioenfonds. Het bestuur benoemt de compliance officer, die onder andere is belast met het toezicht op de naleving van toepasselijke compliance wet- en regelgeving, de gedragscode en diverse compliance reglementen van het fonds. Het bestuur zorgt voor vastlegging van de taken en verantwoordelijkheden van de compliance officer.

6.1. Taken en bevoegdheden

Ten aanzien van de toetsing naleving van de gedragscode zijn de taken en bevoegdheden van de compliance officer als volgt:

- a. de procedurele toetsing van de naleving van de gedragscode;
- b. het controleren van de aanvangsverklaringen, de verklaringen inzake het hebben ontvangen van een aangepaste gedragscode en de jaarlijkse verklaring inzake het naleven van de getekende gedragscode;
- c. het toetsen van het tijdsbeslag van bestuurders (en leden van de raad van toezicht), op basis van gemelde nevenfuncties;
- d. monitoren dat het fonds compliant is met externe compliance wet- en regelgeving en interne regels en procedures;
- e. toetsen van compliance en gelijkwaardige gedragscode bij de uitbestedingspartijen;
- f. het eventueel adviseren van verbonden personen over de uitleg en toepassing van bepalingen zoals die zijn opgenomen in de gedragscode;
- g. het documenteren van zijn werkmethoden en werkzaamheden en het administreren en archiveren van alle informatie die is verstrekt in het kader van de gedragscode(s);
- h. het aanschrijven van insiders en uitvoeren van de toetsing van de insiderregeling (indien van toepassing);
- i. het signaleren van relevante ontwikkelingen en het doen van aanbevelingen aan het bestuur voor implementatie van (gewijzigde) wet- en regelgeving;
- j. het opleggen van eventuele sancties en/of het nemen van maatregelen na een geconstateerde overtreding.

Naast het bovengenoemde, heeft de compliance officer de volgende taken en bevoegdheden:

- a. het doen van aanbevelingen aan het bestuur naar aanleiding van de bevindingen in de jaarlijkse rapportage;
- b. het faciliteren, adviseren en toetsen van het bestuur en manager bij het implementeren en onderhouden van compliance;
- c. het ontvangen, registreren en beoordelen van meldingen van misstanden op grond van de klokkenluidersregeling;
- d. het ontvangen, registreren en beoordelen van meldingen van incidenten op grond van de incidentenregeling;
- e. het registreren van meldingen van overtredingen van verbonden personen en het doen van aanbevelingen inzake te nemen maatregelen of op te leggen sancties;

- f. het opvragen van nadere informatie bij verbonden personen in het kader van de beoordeling van een gedane melding;
- g. het steekproefsgewijs opvragen van informatie bij verbonden personen in het kader van de uitvoering van de compliance werkzaamheden;
- h. het voeren van overleg met het bestuur en/of de manager;
- i. het op verzoek van het bestuur en/of de manager aanvullende werkzaamheden vervullen, zoals het verzorgen van workshops/bewustwordingssessies inzake compliance.

6.2. Rapportage

De compliance officer rapporteert zijn bevindingen jaarlijks aan het dagelijks bestuur. Deze rapportage wordt door het dagelijks bestuur doorgezonden aan de raad van toezicht. Indien en voor zover het om aangelegenheden van de leden van het bestuur gaat, kan de compliance officer ook direct rapporteren aan de raad van toezicht.

De compliance officer rapporteert, inzake medewerkers van het fonds, aan de manager van het fonds.

6.3. Overleg compliance officer

De compliance officer heeft eens per jaar overleg met het bestuur over de gang van zaken met betrekking tot compliance en gedragscode de integere bedrijfsvoering van het fonds en de rol van het bestuur als eindverantwoordelijke daarin.

De compliance officer heeft eens per jaar overleg met de risicomanager van fonds over de geanalyseerde risico's, wijzigingen ten aanzien van integriteitsrisico's die het fonds loopt en het functioneren van het risicomanagementsysteem.

Indien daartoe aanleiding bestaat, kan de compliance officer in onderling overleg met het bestuur dan wel de manager van het fonds een tussentijds overleg inplannen.

6.4. Geheimhouding

De compliance officer en het orgaan of de persoon waaraan hij rapporteert, zijn gehouden tot geheimhouding van informatie verstrekt door verbonden personen of derden. De geheimhouding kan worden doorbroken in het geval een goede uitoefening van zijn functie daartoe noodzaakt.

6.5. Onvoorzien

In geval de reglementen van het fonds niet voorzien in een ontstane situatie overleggen de compliance officer en het bestuur over de te volgen procedure.

7. Uitbesteding

Aangezien SPTN de pensioenadministratie en het vermogensbeheer heeft uitbesteed, zijn hierover afspraken vastgelegd in een overeenkomst met de partijen waaraan deze zijn uitbesteed. Het bestuur van SPTN dient zich er jaarlijks van te vergewissen dat deze partijen handelen conform interne regelgeving en externe wet- en regelgeving.

8. Vaststelling

Dit handboek Compliance is vastgesteld in de bestuursvergadering van 24 september 2021 en laatstelijk gewijzigd per 6 december 2024.

Bijlage 1 Integriteitsbeleid

Bijlage 1 Integriteitsbeleid

1. Inleiding

Integriteit is een wezenlijk kenmerk van een professioneel en betrouwbaar functionerende organisatie. Het bevordert niet alleen de efficiëntie, de interne transparantie en samenwerking, maar ook het vertrouwen.

Het bestuur van Stichting Pensioenfonds Thales Nederland (hierna: SPTN heeft op grond van artikel 19 van het Besluit Financieel Toetsingskader Pensioenfonds (hierna: Besluit FTK) een integriteitsbeleid vastgesteld waarin zij het beleid beschrijft om te komen tot beheersing van de integriteitsrisico's die het pensioenfonds loopt. Dit integriteitsbeleid is in dit document beschreven.

Het onderwerp belangenverstrengeling is ook opgenomen in de Verordening betreffende digitale operationele weerbaarheid (DORA). SPTN beschikt over procedures en maatregelen voor het voorkomen van (de schijn van) van belangenconflicten rondom ICT-dienstverleners en testers, inclusief het permanent monitoren van dergelijke belangenconflicten. Deze procedures en maatregelen zijn opgenomen in het Uitbestedingsbeleid en de Beleidsnotitie ICT van het pensioenfonds.

Met een gedegen integriteitsbeleid tracht SPTN te voorkomen dat het pensioenfonds betrokken raakt bij handelingen die in strijd zijn met de wet of maatschappelijk onbetamelijk zijn. Voor het goed kunnen functioneren als Pensioenfonds is vertrouwen in het fonds een voorwaarde. Integriteit vormt een van de pijlers van het vertrouwen.

Dit integriteitsbeleid zet vooral in op het onderkennen en herkennen van risicosituaties en kan alleen werken wanneer alle betrokken partijen binnen SPTN dit beleid uit kunnen voeren en uitdragen.

2. Doelstelling

De doelstelling van het integriteitsbeleid is het stimuleren dat aan SPTN verbonden personen op alle niveaus handelen in overeenstemming met maatschappelijk geaccepteerde waarden en normen en met de toepasselijke wet- en regelgeving.

Tevens is het doel van het integriteitsbeleid om inzicht te verschaffen aan interne- en externe partijen over de onderkenning van integriteitsrisico's en de genomen beheersmaatregelen.

Het beleid van het pensioenfonds is er op gericht om integriteitsrisico's tot een absoluut minimum beperkt te houden en zo snel mogelijk adequate maatregelen te nemen mocht zich (een kans op het ontstaan van) een integriteitsrisico voordoen. Dit geldt zowel voor de eigen organisatie als voor uitbestedingsrelaties en overige tegenpartijen.

Integriteitsbeleid is daarmee de pijler onder een van de doelstellingen van het pensioenfonds: het hebben van een integere bedrijfsvoering.

3. Reikwijdte van het integriteitsbeleid

Het integriteitsbeleid is van toepassing op de verbonden personen. SPTN heeft de volgende personen als verbonden personen aangemerkt:

- a. leden van het bestuur,
- b. leden van de Raad van Toezicht en het Verantwoordingsorgaan;
- c. externe leden van commissies die zijn ingesteld ter ondersteuning van het bestuur,
- d. medewerkers van het bestuursbureau, waaronder mensen die tijdelijk werken/inhuur,
- e. andere (groepen van) personen die door het bestuur worden aangewezen,
- f. sleutelfunctiehouders en de vervullers van de sleutelfuncties.

Het pensioenfonds heeft de pensioenadministratie en het vermogensbeheer geheel uitbesteed. Medewerkers van uitbestedingspartners zijn geen verbonden personen, tenzij deze op basis van lid e van dit artikel wel als zodanig door het bestuur zijn aangewezen.

Het pensioenfonds hanteert als voorwaarde voor uitbestedingspartners dat zij beschikken over een gedragscode die minimaal gelijkwaardig is aan de gedragscode die het pensioenfonds hanteert dan wel bereid is zich te conformeren aan de gedragscode van het pensioenfonds.

Het handelen door de verbonden persoon in strijd met het integriteitsbeleid en/of 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 en afhankelijk van de aard van de relatie tussen verbonden persoon en pensioenfonds.

4. Integriteitsrisicoanalyse

Het doel van het pensioenfonds is het integriteitsrisico zoveel mogelijk te beperken. Daartoe voert het pensioenfonds periodiek en op systematische wijze een integriteitsrisicoanalyse (SIRA) uit.

Hierbij wordt het volgende proces doorlopen:

- risico-identificatie van reeds bekende integriteitsrisico's en mogelijke nieuwe integriteitsrisico's;
- risicoanalyse bestaande uit een kans/impact analyse (bruto);
- inventarisatie bestaande beheersmaatregelen en indien nodig formuleren van passende aanvullende maatregelen;
- bepalen resterend netto risico;
- monitoren van de risico's en aanpassingen doorvoeren indien nodig.

In 2021 is een SIRA uitgevoerd. De volgende integriteitsrisico's zijn uitgewerkt:

- | | |
|---|---|
| - Belangenverstrengeling | - Ontduiking / ontwijking fiscale regelgeving |
| - Benadeling van derden | - Cybercrime |
| - Handelen met voorwetenschap | - Marktmanipulatie |
| - Witwassen | - Omzeiling sanctiewetgeving |
| - Terrorismefinanciering | - Omkoping |
| - Interne fraude | - Incidenten |
| - Externe fraude | - Uitbesteding |
| - Maatschappelijk onbetamelijk handelen | |

De uitwerking van deze risico's is opgenomen in de bijlage SIRA Integriteitsrisico's vastgesteld 30 november 2021 bij dit beleid.

5. Implementatie beheersmaatregelen en monitoring

De beheersmaatregelen zijn vastgelegd in de SIRA en verankerd in het IRM-beleid.

Naast de beheersmaatregelen per soort risico, neemt het pensioenfonds generieke beheersmaatregelen. Deze zijn verdeeld in *binnen het fonds* en bij *uitbestedingspartijen*.

Binnen het fonds:

- Het fonds beschikt over een handboek Compliance. Hierin zijn onder andere normen opgenomen, waar op regelmatige wijze op wordt getoetst.
- Het fonds beschikt over een gedragscode met daarin gedragsnormen, zoals rondom relatiegeschenken en uitnodigingen. Voor iedere verbonden persoon is er een meldingsplicht. Ook moet iedere verbonden persoon de gedragscode ondertekenen, alsmede een jaarlijkse verklaring. De Compliance Officer heeft een toetsende rol. Er zijn sancties bij handelen in strijd met de gedragscode door verbonden personen. Naast de gedragscode heeft het fonds een klokkenluidersregeling, een incidentenregeling en een privacyregeling. Incidenten worden afgehandeld conform de incidentenregeling.
- Het fonds hanteert een procedure waarbij aan ieder beleidsvoorstel een risicoparagraaf wordt toegevoegd om de risico's inzichtelijk te maken.
- De sponsor traint werknemers actief op het gebied van integriteit en ethiek (awareness). De bestuursleden werken bij de sponsor of hebben bij de sponsor gewerkt. Periodiek is er een sessie met het bestuur voor bewustwording inzake integriteitsrisico's.
- Binnen het bestuur is er ruimte voor discussies over integriteitsvraagstukken, waarbij bestuurders bijvoorbeeld dilemma's bespreekbaar kunnen maken.
- Het fonds houdt zich aan de wettelijke taak en volgt vaak PME wegens de dispensatie, waardoor de ruimte om voor niet-integer handelen beperkt is.
- Bij indiensttreding bij Thales Nederland BV is er een gedegen screening.
- Het verantwoordingsorgaan bestaat uit 6 personen en zij krijgen tevens het advies zelfevaluatie uit te voeren waardoor men elkaar kan aanspreken op gedrag en er een open cultuur heerst.
- Externe verbonden personen worden na een zorgvuldig selectieproces aangesteld.

Bij uitbestedingspartijen:

- Bij aangaan van een uitbestedingsrelatie wordt getoetst dat de gedragscode minimaal net zo zwaar is als de gedragscode van SPTN. Contractueel is vastgelegd dat incidenten worden gemeld. De ISAE verklaringen worden getoetst. Uitbestedingspartijen hebben de contractuele plicht om incidenten te melden. Als er door uitbestedingspartijen incidenten worden gemeld, dan worden deze binnen het fonds besproken en wordt bepaald of maatregelen nodig zijn.

- (kritieke) uitbestedingspartijen hebben een procuratieregeling en hanteren functiescheiding.
- De uitbestedingspartijen hanteren m.b.t. besluitvorming het 4-ogenprincipe.

De Compliance Officer en risicomanager voeren controles uit op de genomen beheersmaatregelen en rapporteren respectievelijk jaarlijks en halfjaarlijks aan het bestuur van het pensioenfonds over de status en effectiviteit van de beheersmaatregelen.

6. Rapportage

Over beheersing van integriteitsrisico's legt het bestuur van SPTN verantwoording af aan:

- de toezichthouder (indien nodig)
- Raad van Toezicht
- Verantwoordingsorgaan
- Compliance Officer

Het borgen van de compliance aspecten van uitbestede activiteiten gebeurt door heldere afspraken te maken met contractpartijen (o.a. door middel van SLA-afspraken en rapportages). SPTN ontvangt ieder jaar een verklaring van externe partijen waarbij zij verklaren dat ze het afgelopen jaar compliant zijn geweest en een gedragscode hanteren die minimaal gelijkwaardig is aan de gedragscode van SPTN. Integriteitsrisico's zijn hier een onderdeel van.

Indien er wijzigingen zijn aan de gestelde eisen worden de externe partijen via de jaarlijkse correspondentie op de hoogte gesteld. Er worden bezoeken op locatie van de externe partijen afgelegd.

Tevens worden de ISAE 3402 rapporten (kwaliteit van de interne rapporten en processen en naleving van processen) van de vermogensbeheerders, custodian en pensioenadministratie jaarlijks beoordeeld.

7. Bewustwording/bewustzijn

Vertrouwen is cruciaal en van doorslaggevend belang voor het functioneren van een pensioenfonds. Integriteit en openheid zijn een absolute voorwaarde om het vertrouwen van deelnemers en werkgevers te winnen en te behouden.

Daarbij is bewustwording van essentieel belang. Bewustwording is gericht op het veranderen en verbeteren van kennis, houding en gedrag van medewerkers en bestuur ten aanzien van externe wet- en regelgeving en interne procedures en (gedrags)regels. Dit is essentieel omdat het, zonder het juiste gedrag van medewerkers en bestuur, niet effectief is om beheersmaatregelen in te voeren om de integriteit van SPTN te garanderen.

Bewustwording met betrekking tot de integriteitsrisico's vergt training van zowel bestuur als medewerkers. SPTN leeft de hoogst zakelijke normen en waarden na en waarborgt deze zodat integriteit doordringt tot in de bedrijfscultuur, processen en beslissingen. Op verzoek van het bestuur en/of manager Pensioenfonds verzorgt de Compliance Officer een workshop hiertoe.

Uitgangspunt is dat iedere verbonden persoon bij SPTN een eigen verantwoordelijkheid heeft voor de integere bedrijfscultuur en naleving van de relevante wet- en regelgeving. Van de verbonden personen wordt derhalve verwacht dat zij:

- Kennis hebben van de betekenis, het nut en de noodzaak van integriteitsrisico's in het algemeen en de wijze waarop SPTN daar invulling aan geeft;
- Kennis hebben van de belangrijkste wet- en regelgeving en interne gedragsregels en procedures met betrekking tot integriteitskwesaties;
- Vermeende ongewenste gedragingen en incidenten leren herkennen en signaleren en weten welke procedures in geval van een incident moeten worden gehanteerd.

8. Integere deelnemer bediening

Vanuit de invalshoek van deelnemers is het belangrijk dat SPTN een betrouwbare dienstverlener is. Betrouwbaar houdt onder andere in dat de deelnemer op een correcte manier wordt behandeld en juist wordt geïnformeerd over de producten die worden aangeboden. Dit omvat vele aspecten die gebaseerd zijn op wet- en regelgeving.

Het bestuur van SPTN heeft een beleid opgesteld van procedures over de communicatie aan deelnemers (het inbouwen van kwaliteitswaarborgen). Er is een communicatiecommissie ingesteld die meerdere keren per jaar bijeenkomt.

Er wordt aantoonbaar verantwoording afgelegd aan de deelnemers middels een verantwoordingsorgaan, Raad van Toezicht en een heldere verslaglegging.

Tevens geeft het bestuur openheid door het geven van een toelichting op het gevoerde beleid in de jaarlijkse informatiebijeenkomst.

9. Overige regelingen

Incidenten

SPTN heeft een incidenten- en klokkenluidersregeling (zie bijlage 3 en 4).

Regeling ongewenst gedrag

Voor de regeling “ongewenst gedrag” wordt verwezen naar het beleid van Thales NL (“ongewenste omgangsvormen”).

10. Inwerkingtreding

Dit Integriteitsbeleid is laatstelijk gewijzigd en vastgesteld op 6 december 2024 en treedt per die datum in werking.

SIRA Integriteitsrisico's vastgesteld 30 november 2021

Sub- risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 1 Belangenverstrengeling	3	3	9	- In de gedragscode zijn normen opgenomen ten aanzien van belangenconflicten, met daarin specifieke regels bij een aantal expliciet benoemde gevallen, waarin sprake kan zijn van (de schijn van) een potentieel belangenconflict. - In het uitbestedingsbeleid en de Beleidsnotitie ICT van het fonds zijn bepalingen opgenomen in het kader van belangenverstrengeling. Hierin wordt verwezen naar de normen en wordt het proces geschetst bij (de schijn van) belangenverstrengeling in selectietrajecten. - Daar waar mogelijk (de schijn van) belangenverstrengeling een rol speelt (bijvoorbeeld door het paritaire model), worden bewust keuzes gemaakt om bepaalde functionarissen geen deel uit te laten maken van de besluitvorming. Het bestuur toetst elkaar hierop en laten zich ook toetsen. - De afgesloten vermogensbeheerovereenkomsten bieden geen mogelijkheid invloed uit te oefenen op de afzonderlijke transacties in financiële instrumenten. Er zijn geen clausules in de vooraf overeengekomen mandaten, waarbij de vermogensbeheerder onder bepaalde voorwaarden toestemming moet vragen voordat er transacties mogen worden verricht in (bepaalde) financiële instrumenten. - Bestuurders of andere bij het fonds betrokken personen hebben geen enkele invloed op de afzonderlijke transacties in financiële instrumenten. - Er is ook geen enkel vermoeden in welke afzonderlijke financiële instrumenten Er belegd wordt omdat Er geen instructies worden gegeven en Er anderszijds geen link is te leggen met eventuele bedragen die worden overgemaakt.	2	2	4	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
vervolg Belangenverstrengeling	3	3	9	- in de vermogensbeheerovereenkomsten is het beleggingsbeleid verder ook niet ingevuld met financiële instrumenten van een (beperkt) aantal specifieke vennootschappen. - de verbonden personen beschikken niet over koersgevoelige informatie of over informatie waarvan zij weten of redelijkerwijs moeten vermoeden dat deze informatie als koersgevoelig moet worden aangemerkt. - het pensioenfonds verricht geen transacties voor eigen rekening in financiële instrumenten. - Verstrengeling van belangen tussen een tester van tests van digitale operationele weerbaarheid en de ICT-dienstverlener van SPTN waar de tests worden uitgevoerd worden tijdens de selectietraject onderzocht. - Monitoring van het risico van belangenverstrengeling vindt plaats binnen het bestuur, met ondersteuning van de compliance officer.	2	2	4	Ja
Risico 2 Benadeling van derden	3	3	9	- Het fonds heeft de normen voor selectieprocedures vastgelegd in het uitbestedingsbeleid. In een selectietraject worden altijd meerdere partijen benaderd die dezelfde informatie ontvangen. (Potentiële) uitbestedingspartijen mogen niet rechtstreeks contact opnemen met een bestuurder. Dilemma's worden open en transparant besproken in het bestuur.	2	2	4	Ja
Risico 3 Handelen met voorwetenschap	1	1	1	- Bestuurders of andere bij het fonds betrokken personen hebben geen enkele invloed op de afzonderlijke transacties in financiële instrumenten. - Bestuurders of andere bij het fonds betrokken personen komen niet in aanraking met niet-openbare informatie, doordat het vermogensbeheer volledig is uitbesteed aan een vermogensbeheerder (BlackRock) met een balanced mandaat zoals jaarlijks vastgelegd in de beleggingsrichtlijnen. - De vermogensbeheerder heeft beleid en procedures voor dit risico. Dit wordt gemonitord en gerapporteerd. Ook zijn er procedures bij incidenten en worden incidenten gemeld aan het fonds.	1	1	1	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 4 Witwassen	2	4	8	- Er is een procuratieoverzicht opgesteld, waarbij geldt dat voor transacties altijd een bestuurder van werkgeverszijde tekent, tezamen met een bestuurder van werknemerszijde. - De inkomende geldstromen van het pensioenfonds beperken zich bijna volledig door premie-inkomsten die afkomstig zijn van de sponsor. - In het selectieproces voor uitbestedingen wordt een risicoanalyse uitgevoerd. - Minimaal elke 2 jaar vindt een uitbestedingsrisicoanalyse plaats. Hierin worden onder andere de processen beoordeeld die fraude moeten tegengaan (zoals functiescheiding verwerken beleggings- en banktransacties, pre-employment screening).- Er zijn betalingsprocedures bij uitbestedingspartijen, waarbij onder andere gescreeend wordt op verdachte transacties. - Er zijn procedures bij uitbestedingspartijen m.b.t. het screenen en monitoren van relaties/ medewerkers en (onder)uitbestedingspartijen.	1	4	4	Ja
Risico 5 Terrorismedinanciering	2	4	8	- Er wordt door alle uitbestedingspartijen (zoals de pensioenuitvoerder en vermogensbeheerder) actief gescreeend op terrorismefinanciering. De (inter)nationale sanctielijsten worden hierbij up-to-date gehouden en gehanteerd. Bij zogenaamde hits wordt er gerapporteerd aan het fonds. Bovendien worden in dit geval tegemoeten van de personen en/of partijen bevroren. Dit wordt gemonitord door het fonds.	1	4	4	Ja, met inachtneming aanvullende maatregelen.
Aanvullende maatregelen: - Controleren of dit contractueel is vastgelegd bij alle uitbestedingspartijen of zo spoedig mogelijk contractueel vastleggen daar waar dit nog niet is vastgelegd.								
Risico 6 Interne fraude	2	2	4	- Er is een procuratieoverzicht opgesteld, waarbij geldt dat voor transacties altijd een bestuurder van werkgeverszijde tekent, tezamen met een bestuurder van werknemerszijde. - De inkomende geldstromen van het pensioenfonds beperken zich bijna volledig door premie-inkomsten die afkomstig zijn van de sponsor. - Monitoring van dit risico vindt plaats binnen het bestuur.	1	2	2	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 7 Externe fraude	3	2	6	- Declaraties worden alleen goedgekeurd met specificatie van gewerkte uren of diensten. Autorisatie conform 4-ogen principe. - Het fonds werkt met liquiditeitsprognoses, afwijkingen worden geëvalueerd waardoor externe fraude kan worden geïdentificeerd. - In het selectieproces voor uitbestedingen wordt een risicoanalyse uitgevoerd. - Minimaal elke jaar vindt een uitbestedingsrisicoanalyse plaats. Hierin worden onder andere de processen beoordeeld die fraude moeten tegengaan (zoals functiescheiding verwerken beleggings- en banktransacties, pre-employment screening, beloningsbeleid). - Het uitbestedingsbeleid bevat normen voor uitbestedingsrelaties (zoals certificeringen). Deze normen zijn voorafgaan aan de relatie getoetst en worden gedurende de relatie geëvalueerd. - Jaarlijkse beoordeling ISAE verklaring, waarbij het betalingsproces en het transactieproces in scope zijn. - Jaarlijkse accountantscontrole uitbestedingspartijen. - Monitoring van dit risico vindt plaats binnen het bestuur.	2	2	4	Ja, met inachtneming aanvullende maatregelen.
Aanvullende maatregelen: - Checks bij GBA of opvragen attestatie de vitae - Controleren of de normen en mogelijke consequenties wanneer normen niet gehaald worden contractueel zijn vastgelegd bij alle uitbestedingspartijen of zo spoedig mogelijk contractueel vastleggen daar waar dit nog niet is vastgelegd.								
Risico 8 Maatschappelijk onbetamelijk handelen	3	3	9	- Screening van medewerkers van Thales Nederland bv. - Er is een procuratieoverzicht opgesteld. Transacties worden altijd getekend door twee bestuursleden, zoals beschreven onder inventarisatie van mogelijke maatregelen. - Het fonds beschikt over een MVB-beleid en ESG-beleid. - Selectieproces voor uitbestedingen met een risicoanalyse. - Monitoring van dit risico vindt plaats binnen het bestuur.	2	3	6	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 9 Ontduiking / ontwijking fiscale regelgeving	2	3	6	- Jaarlijkse accountantscontrole bij het fonds en bij uitbestedingspartijen. - Het fonds stuurt niet actief op terugvorderingen. - In het selectieproces voor uitbestedingen wordt een risicoanalyse uitgevoerd. - Minimaal elke 2 jaar vindt een uitbestedingsrisicoanalyse plaats. - Het uitbestedingsbeleid bevat normen voor uitbestedingsrelaties (zoals certificeringen). Deze normen zijn voorafgaand aan de relatie getoetst en worden gedurende de relatie geëvalueerd. De normen zijn contractueel vastgelegd. Wanneer de normen niet gehaald worden, is er een consequentie overeengekomen.	1	3	3	Ja
Risico 10 Cybercrime	4	4	16	- Het fonds heeft een ICT-beleid, voorzien van normen voor cybersecurity bij uitbestedingspartijen. Periodiek wordt het fonds door de uitvoeringspartijen geïnformeerd over het gevoerde cybersecurity beleid en de beheersing van de cyber risico 's. Het fonds stelt verder als eis dat de uitvoeringspartijen voldoen aan de wet- en regelgeving op dit gebied zoals de Europese cybersecurityrichtlijn over Netwerk en Informatiebeveiliging (de NIB-richtlijn). Ook stelt het fonds als eis dat de uitvoeringspartijen voldoen aan de vier extra Cobitcontrols die door DNB specifiek voor cybersecurity zijn toegevoegd. - In het selectieproces voor uitbestedingen wordt een risicoanalyse uitgevoerd. Bij het aangaan van de uitbestedingsrelatie is de IT organisatie van de uitbestedingsrelatie beoordeeld. - Met Appel is een verwerkersovereenkomst gesloten. Met onderuitbestedingen is door Appel ook een verwerkingsovereenkomst gesloten. - Minimaal elke jaar vindt een uitbestedingsrisicoanalyse plaats, waarin ook de IT organisatie wordt betrokken. - Het uitbestedingsbeleid bevat normen voor uitbestedingsrelaties (zoals certificeringen). Deze normen zijn voorafgaand aan de relatie getoetst en worden gedurende de relatie geëvalueerd.	3	3	9	Ja, met inachtneming aanvullende maatregelen.

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
vervolg Cybercrime	4	4	16	De normen zijn contractueel vastgelegd. Wanneer de normen niet gehaald worden, is er een consequentie overeengekomen. - Periodiek uitdraag en beoordeling self assessment informatiebeveiligingsraamwerk. - Jaarlijkse beoordeling ISAE 3402 en ISAE 3000 en ISO. - Op kwartaalbasis beoordeling en bespreking SLA rapportage. - Als de uitbestedingspartij niet in control is; Contractueel is bepaald dat een verbeterplan in werking treedt wanneer de uitbestedingspartij in gebreke is. Dit plan moet in werking worden gezet. Adequaat reageren door tijdig melding van gebrek(en) te maken. Monitoren verbeterplan. - Data wordt versleuteld uitgewisseld door het fonds en uitbestedingspartijen. - Interfaces uitbestedingspartijen zijn voorzien van een SSL of TLS-certificaat. - Appel en de vermogensbeheerder voeren periodiek patch-, vulnerability-, en pentesten uit. - Uitbestedingspartijen hanteren een autorisatiebeleid en beoordelen toegekende autorisaties periodiek op juistheid en volledigheid. - Vertrouwelijke stukken worden beveiligd gedeeld.	3	3	9	Ja, met inachtneming aanvullende maatregelen.
Aanvullende maatregelen - IT landschap uitbestede partijen in kaart brengen en opstellen plan van aanpak voor betere beheersing van de risico's.								
Risico 11 Marktmanipulatie	3	3	9	- Bestuurders of andere bij het fonds betrokken personen hebben geen enkele invloed op de afzonderlijke transacties in financiële instrumenten. - Bestuurders of andere bij het fonds betrokken personen komen niet in aanraking met niet-openbare informatie, doordat het vermogensbeheer volledig is uitbesteed aan een vermogensbeheerder (BlackRock) met een balanced mandaat zoals jaarlijks vastgelegd in de beleggingsrichtlijnen. - De vermogensbeheerder heeft beleid en procedures voor dit risico. Dit wordt gemonitord en gerapporteerd. Ook zijn er procedures bij incidenten en worden incidenten gemeld aan het fonds.	2	2	4	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 12 Omzeiling sanctiewetgeving	2	3	6	- Er wordt door Appel en Blackrock actief gescreend op (inter)nationale sanctielijsten. De (inter)nationale sanctielijsten worden hierbij up-to-date gehouden en gehanteerd. Bij zogenaamde hits wordt er gerapporteerd aan het fonds. Bovendien worden in dit geval tegoeden van de personen en/of partijen bevroren. Dit is contractueel vastgelegd en wordt gemonitord door het fonds.	1	3	3	Ja
Risico 13 Omkoop	2	2	4	- De afgesloten vermogensbeheerovereenkomsten bieden geen mogelijkheid invloed uit te oefenen op de afzonderlijke transacties in financiële instrumenten. Er zijn geen clausules in de vooraf overeengekomen mandaten, waarbij de vermogensbeheerder onder bepaalde voorwaarden toestemming moet vragen voordat er transacties mogen worden verricht in (bepaalde) financiële instrumenten. - Bestuurders of andere bij het fonds betrokken personen hebben geen enkele invloed op de afzonderlijke transacties in financiële instrumenten. - Er is ook geen enkel vermoeden in welke afzonderlijke financiële instrumenten er belegd wordt omdat er geen instructies worden gegeven en er anderszids geen link is te leggen met eventuele bedragen die worden overgemaakt. - In de vermogensbeheerovereenkomsten is het beleggingsbeleid verder ook niet ingevuld met financiële instrumenten van een (beperkt) aantal specifieke vennootschappen. - De verbonden personen beschikken niet over koersgevoelige informatie of over informatie waarvan zij weten of redelijkerwijs moeten vermoeden dat deze informatie als koersgevoelig moet worden aangemerkt. - Het pensioenfonds verricht geen transacties voor eigen rekening in financiële instrumenten. - Hanteren van het 4-ogen principe bij besluiten en transacties. - Monitoring van het risico vindt plaats binnen het bestuur, met ondersteuning van de compliance officer.	1	2	2	Ja

Sub-risico	Kans	Impact	Gevolg (K*I)	Beheersmaatregelen	Kans	Impact	Gevolg (K*I)	Restrisico acceptabel
Risico 14 Incidenten	3	2	6	[Algemene maatregelen, zoals open cultuur, en klokkenluiders- en incidentenregelingen, meldplicht]	2	2	4	Ja
Risico 15 Uitbesteding	3	2	6	- In het selectieproces voor uitbestedingen wordt een risicoanalyse uitgevoerd. - Het uitbestedingsbeleid bevat normen voor uitbestedingsrelaties (zoals certificeringen). Deze normen zijn voorafgaan aan de relatie getoetst en worden gedurende de relatie geëvalueerd. - Met uitbestedingspartijen worden SLA's vastgesteld.	2	1	2	Ja, met inachtneming aanvullende maatregelen.

Aanvullende maatregelen:

- Controleren of de normen en mogelijke consequenties wanneer normen niet gehaald worden contractueel zijn vastgelegd bij alle uitbestedingspartijen of zo spoedig mogelijk contractueel vastleggen daar waar dit nog niet is vastgelegd.

Bijlage 2 Gedragscode Pensioenfonds Thales Nederland

Hoofdstuk 1 Definities

1.1 Verbonden personen zijn:

- a. leden van het bestuur,
- b. leden van de Raad van Toezicht/ Visitatiecommissie en het Verantwoordingsorgaan/Belanghebbendenorgaan;
- c. externe leden van commissies die zijn ingesteld ter ondersteuning van het bestuur,
- d. medewerkers van het bestuursbureau, waaronder mensen die tijdelijk werken/inhuur,
- e. andere (groepen van) personen die door het bestuur worden aangewezen.

Medewerkers van uitbestedingspartners zijn geen verbonden personen, tenzij deze op basis van lid e van dit artikel wel als zodanig door het bestuur zijn aangewezen.

1.2 Insiders zijn:

verbonden personen, die direct of indirect bij transacties van het pensioenfonds in financiële instrumenten zijn betrokken, dan wel anderszins uit hoofde van hun werkzaamheden, beroep of functie over voorwetenschap beschikken of kunnen beschikken. Een insider is ook de verbonden persoon die kan beschikken over andere vertrouwelijke (markt)informatie. Het bestuur kan andere (groepen van) verbonden personen als insider aanwijzen. Het bestuur stelt een verbonden persoon schriftelijk op de hoogte als hij wordt aangemerkt als insider.

1.3 Gelieerde derden zijn:

- a. echtgenoot, echtgenote of partner van de verbonden persoon,
- b. bloed- en aanverwanten tot de tweede graad van de verbonden persoon,
- c. (andere) personen die tot hetzelfde huishouden als de verbonden persoon behoren,
- d. lasthebbers en vermogensbeheerders (niet zijnde vrije hand beheerders), voor zover handelend ten behoeve van de verbonden persoon,
- e. rechts-of natuurlijke personen met wie de verbonden persoon een relatie heeft welke van dien aard is dat de verbonden persoon een direct of indirect wezenlijk belang heeft bij het resultaat van een transactie in een financieel instrument.

1.4 Persoonlijke transactie is:

- a. een transactie in een financieel instrument, door of in naam van een insider, waarbij:
 - 1. de insider handelt anders dan in de normale uitoefening van zijn beroep of functie,
 - 2. een transactie wordt verricht voor rekening van de insider, of
 - 3. een transactie wordt verricht voor rekening van gelieerde derden, dan wel
 - b. een andersoortige (financiële) transactie, inclusief het anders dan in de normale uitoefening van zijn beroep of functie verrichten, doen verrichten of bewerkstelligen van enige handeling, ten voordele van de insider of gelieerde derden.
- 1.5 Onder financieel instrument worden begrepen:
- a. effect,
 - b. geldmarktinstrument,
 - c. recht van deelneming in een beleggingsinstelling, niet zijnde een effect,
 - d. derivatencontract, waaronder begrepen maar daartoe niet beperkt een optie, future, swap, valuta-en rentetermijncontract,
 - e. overige financiële instrumenten in de zin van de Wet op het financieel toezicht, en voorts al hetgeen naar de opvattingen in het maatschappelijk verkeer als zodanig wordt beschouwd.
- 1.6 Integriteitsrisico is:
gevaar voor de aantasting van de goede reputatie, alsmede de bestaande en toekomstige bedreiging van het vermogen of resultaat van het pensioenfonds.
- 1.7 Reputatierisico is:
gevaar voor de aantasting van de goede reputatie van het pensioenfonds.
- 1.8 Voorwetenschap is:
de bekendheid met informatie die concreet is en die rechtstreeks of middellijk betrekking heeft op een uitgevende instelling, waarop de financiële instrumenten betrekking hebben, of omtrent de handel in deze financiële instrumenten, welke informatie niet openbaar is gemaakt en waarvan openbaarmaking significante invloed zou kunnen hebben op de koers van de financiële instrumenten of op de koers van daarvan afgeleide financiële instrumenten.
- 1.9 Compliance is:
het bewerkstelligen van een integere bedrijfsvoering van het pensioenfonds en een integere cultuur waar het als vanzelfsprekend is dat

verbonden personen handelen in overeenstemming met de geldende maatschappelijke normen en de wet- en regelgeving.

- 1.10 Compliance Officer:
De door het Bestuur van Stichting Pensioenfonds Thales Nederland aangewezen medewerker die is belast met het houden van toezicht op en de bevordering van compliance.
- 1.11 Nevenfunctie is:
iedere functie die een Verbonden Persoon verricht naast zijn functie bij het pensioenfonds.
- 1.12 Andere vertrouwelijke (markt)informatie is:
Informatie die door haar aard of inhoud als zelfstandig gegeven of in combinatie met andere gegevens tot een informatievoorsprong (voorwetenschap) kan leiden voor de Verbonden Persoon of een gelieerde derde. Daarbij is het niet relevant of deze personen werkzaam zijn voor het pensioenfonds of dat deze personen elders werkzaam zijn.
- 1.13 Zakelijke contacten zijn:
partijen van wie het pensioenfonds tegen betaling diensten afneemt, waaronder begrepen leveranciers en dienstverleners.
- 1.14 Belangenconflicten zijn:
wanneer persoonlijke of professionele belangen, anders dan die van het Pensioenfonds, worden meegenomen in de besluitvorming.
- 1.15 Pensioenfonds is:
Stichting Thales Pensioenfonds Nederland
- 1.16 Bestuur is:
het bestuur van de Stichting Pensioenfonds Thales Nederland
- 1.17 Raad van Toezicht/Visitatiecommissie is:
De door het Bestuur aangewezen Raad van Toezicht/ Visitatiecommissie die belast is met het intern toezicht.
- 1.18 Waar in deze gedragscode staat geschreven 'hij' of 'zijn' moet tevens worden gelezen 'zij' of 'haar'.
- 1.19 Indien volgens deze gedragscode de voorzitter van het bestuur toestemming of goedkeuring nodig heeft, wordt toestemming gevraagd aan de vicevoorzitter en/of de compliance officer.

Hoofdstuk 2 Inleidende bepalingen

- 2.1 Het doel van de gedragscode is het waarborgen en handhaven van het vertrouwen van belanghebbenden in het pensioenfonds, door gewenst gedrag te stimuleren en ongewenst gedrag te voorkomen. De gedragscode kent daartoe algemene gedragsregels voor verbonden personen en aanvullende gedragsregels voor insiders.
- 2.2 Naast de gedragscode zijn er vereisten vanuit de Verordening betreffende de digitale operationele weerbaarheid (DORA) rondom het onderwerp belangenverstrengeling. Het pensioenfonds dient te beschikken over procedures en maatregelen voor het voorkomen van (de schijn van) van belangenverstrengeling rondom ICT-dienstverleners en testers, inclusief het permanent monitoren van dergelijke belangenverstrengeling. Deze procedures en maatregelen zijn opgenomen in het Uitbestedingsbeleid en het ICT-beleid van het pensioenfonds.
- 2.3 De gedragscode bevordert de transparantie rondom gedragsregels en maakt duidelijk aan alle bij het pensioenfonds verbonden personen – ook voor de bescherming van hun eigen belangen – wat wel en wat niet is geoorloofd.
- 2.4 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.
- 2.5 De organisatie waaraan het pensioenfonds werkzaamheden heeft uitbesteed, dan wel wordt ingehuurd voor essentiële werkzaamheden van het pensioenfonds, moet beschikken over een gedragscode (inclusief een Insiderregeling voor relevante groepen) die op uitgangspunten gelijkwaardig is aan die van het pensioenfonds.
- 2.6 De hoogste leiding van het pensioenfonds is verantwoordelijk voor het naleven van de verplichtingen die voortvloeien uit enige wettelijke bepaling of de gedragscode.

Hoofdstuk 3 Normen

- 3.1 Van iedere Verbonden Persoon wordt verwacht dat hij zich onder alle omstandigheden zal gedragen volgens de hoogste normen van het pensioenfonds.

De Verbonden Persoon:

- a** voorkomt dat zijn privébelangen in conflict komen dan wel verstrengeld raken met de belangen van het pensioenfonds, dan wel dat de schijn hiervan wordt gewekt. Dit geldt ook bij alle contacten met derden;
- b** vermijdt het gebruik van voorwetenschap of andere vertrouwelijke (markt)informatie dan wel van misbruik en oneigenlijk gebruik van bij het pensioenfonds voorhanden zijnde vertrouwelijke informatie;

- c voorkomt koersmanipulatie en andere misleidende handelingen;
 - d gaat op een uiterst zorgvuldige wijze om met de (persoons)gegevens waar hij de beschikking over heeft of kan hebben.
- 3.2 Van iedere Verbonden Persoon wordt verwacht dat hij zich bewust is van het risico van corruptie. De Verbonden Persoon zal zich niet inlaten met omkoping of enige andere vorm van corruptie.
- 3.3 Het is niet toegestaan derden te betrekken bij handelingen die in strijd zijn met de gedragscode.
- 3.4 Het is niet toegestaan de normen van de gedragscode te omzeilen door het betrekken van (gelieerde) derden.

Hoofdstuk 4 Algemene verplichtingen Verbonden Personen

4.1 Belangenconflicten

De verbonden persoon draagt er zorg voor iedere situatie die aanleiding geeft of zou kunnen geven tot een belangenconflict, te vermijden. De verbonden persoon is verplicht elk (potentieel) belangenconflict direct te melden aan de compliance officer. Voor de volgende gevallen, waarin sprake kan zijn van (de schijn van) een potentieel belangenconflict, gelden specifieke regels:

1. relatiegeschenken;
2. uitnodigingen;
3. nevenfuncties;
4. zakelijke belangen;
5. pensioenfondseigendommen en bedrijfsmiddelen;
6. (aspirant) leveranciers en dienstverleners.

Uitgangspunt in alle gevallen van mogelijke belangenconflicten is dat iedere verbonden persoon een eigen verantwoordelijkheid heeft richting het pensioenfonds en de belanghebbenden van het pensioenfonds. Iedere verbonden persoon moet ervan doordrongen zijn dat (de schijn van) belangenverstrengeling de reputatie van het Pensioenfonds maar ook van de verbonden persoon zelf kan schaden.

4.1.1 Relatiegeschenken andere schenkingen

De verbonden persoon gaat terughoudend en transparant om met het aanvaarden van relatiegeschenken aan hemzelf, of aan Gelieerde Derden. Om te voorkomen dat (de schijn ontstaat dat) het aanvaarden van een relatiegeschenk van invloed kan zijn op beslissingen van het

Pensioenfonds. Het ontvangen van relatiegeschenken door een verbonden persoon is toegestaan onder de volgende voorwaarden:

- relatiegeschenken van één bedrijf of instelling tot maximale waarde van € 50 per jaar,
- zo spoedig mogelijke melding van alle aangeboden geschenken met een waarde van meer dan € 50 aan de voorzitter van het Pensioenfonds, en
- onmiddellijke melding van mogelijke beïnvloeding door (toekomstige) relaties van het Pensioenfonds aan de voorzitter van het Pensioenfonds.

Indien het bestuur van het Pensioenfonds het opportuun acht zelf relatiegeschenken te geven, mag de waarde in beginsel daarvan niet meer zijn dan € 50 per relatie per jaar. Geschenken met een waarde van meer dan € 50 dienen bij de voorzitter gemeld te worden. Het is niet toegestaan relatiegeschenken te geven om daarmee toekomstige beslissingen van derden te beïnvloeden.

4.1.2 Uitnodigingen

Uitgangspunten voor uitnodigingen zijn:

1. ontvangen uitnodigingen worden altijd gemeld aan de voorzitter van het Pensioenfonds;
 2. er wordt terughoudend omgegaan met repeterende uitnodigingen.
- a. Reizen en bedrijfsbezoeken
Uitnodigingen voor reizen en bedrijfsbezoeken mogen worden aanvaard indien:
- er geen sprake is van een potentieel belangenconflict,
 - het zakelijke karakter en het belang voor het Pensioenfonds wordt aangetoond, en
 - de uitnodiging vooraf is goedgekeurd door de voorzitter van het Pensioenfonds.
- b. Congressen/seminars
Uitnodigingen voor congressen/seminars mogen worden aanvaard indien:
- er geen sprake is van een potentieel belangenconflict,
 - de uitnodiging vooraf is goedgekeurd door de voorzitter van het Pensioenfonds.
- c. Evenementen
Uitnodigingen voor evenementen (bijvoorbeeld sportwedstrijden en concerten) mogen worden aanvaard indien:
- er geen sprake is van een potentieel belangenconflict,

- het zakelijke karakter en het belang voor het Pensioenfonds wordt aangetoond, en
 - de uitnodiging vooraf is goedgekeurd door de voorzitter van het Pensioenfonds.
- d. Spreker congres
- Uitnodigingen om als spreker op te treden op een congres of seminar mogen worden aanvaard indien:
- er geen sprake is van een potentieel belangenconflict,
 - de eventuele beloning in verhouding staat met de verrichte werkzaamheden, en
 - de uitnodiging vooraf is goedgekeurd door de voorzitter van het Pensioenfonds.

4.1.3 Nevenfuncties

Het aanvaarden of continueren van een nevenfunctie van een verbonden persoon is toegestaan na goedkeuring door de voorzitter van het Pensioenfonds.

Bij de beoordeling wordt getoetst of sprake is van een nevenfunctie welke

- de schijn heeft, of kan opwekken, van een belangenconflict,
- onevenredige tijdsbesteding met zich meebrengt ten opzichte van de taak bij het Pensioenfonds,
- kan leiden tot reputatieschade voor het Pensioenfonds.

De verbonden persoon doet tevens melding van de nevenfunctie aan de compliance officer door middel van de jaarlijkse verklaring "Naleving gedragscode".

4.1.4 Financiële belangen in zakelijke relaties

Het, al dan niet via een gelieerde derde, houden van een financieel belang in een bedrijf of instelling waarmee het pensioenfonds een zakelijke relatie onderhoudt, of mogelijk zaken gaat doen, is in verband met een (potentieel) belangenconflict niet toegestaan.

4.1.5 Pensioenfondseigendommen

De verbonden persoon gaat zorgvuldig om met de bedrijfsmiddelen van het pensioenfonds. Privégebruik van bedrijfsmiddelen is niet toegestaan zonder voorafgaande toestemming van de voorzitter van het Pensioenfonds. Voorbeelden zijn intellectueel eigendom, kantoorbenodigdheden, computers en computerprogramma's.

4.1.6 Leveranciers en dienstverleners

Het is de verbonden persoon niet toegestaan als privépersoon transacties aan te gaan of privé gebruik te maken van diensten van leveranciers en zakelijke dienstverleners, waarmee het pensioenfonds direct of indirect zakelijke contacten onderhoudt, tenzij als dit algemeen gebruikelijk is, de diensten tegen marktconforme voorwaarden worden uitgevoerd en geldelijk privévoordeel is uitgesloten.

4.1.7. Overige handelingen en transacties

Besluiten tot het aangaan van handelingen en/of transacties waarbij tegenstrijdige belangen van één of meer Verbonden Personen spelen die van materiële of anderszins relevante betekenis zijn voor het Pensioenfonds en/of voor Insiders behoeven voorafgaande schriftelijke goedkeuring van de Voorzitter van het Bestuur, op advies van de Compliance Officer. Dergelijke transacties worden gepubliceerd in het bestuursverslag.

4.1.8 Melding belangenconflict

Iedere Verbonden Persoon is verplicht elk (potentieel) tegenstrijdig belang of reputatierisico te melden aan de Compliance Officer en de voorzitter van het Bestuur. Pogingen van een (aspirant-)relatie tot beïnvloeding zullen eveneens onmiddellijk worden gemeld.

4.2 Voorwetenschap

4.2.1 De verbonden persoon mag geen gebruik maken van voorwetenschap. De verbonden persoon dient verder uiterste zorgvuldigheid te betrachten bij de behandeling van informatie waarvan hij weet of redelijkerwijs behoort te weten dat deze informatie moet worden aangemerkt als vertrouwelijke (markt)informatie. Het gebruik van voorwetenschap en het verspreiden van andere vertrouwelijke informatie is slechts toegestaan indien een zorgvuldige uitoefening van zijn functie dat vereist.

4.2.2 De verbonden persoon die met betrekking tot financiële instrumenten over informatie beschikt als bedoeld in artikel 3.2.1, onthoudt zich van het verrichten van transacties of het aanzetten tot het verrichten van transacties, zowel rechtstreeks als middellijk, in die financiële instrumenten, dan wel van het daarover te adviseren, anders dan van hem bij een zorgvuldige uitoefening van zijn functie mag worden verwacht.

4.2.3 Het is de verbonden persoon verboden om binnen vierentwintig uur opdracht te geven tot zowel een aan-als verkooporder voor transacties in een financieel instrument van dezelfde uitgevende instelling, rechtspersoon of vennootschap.

4.2.4 Het is de verbonden persoon verboden om transacties in een financieel instrument te (laten) verrichten naar aanleiding van of vooruitlopend op effectenorders van het pensioenfonds.

4.2.5 De verbonden persoon, anders dan de insider, die beschikt over informatie als bedoeld in artikel 3.2.1 rapporteert dit aan de compliance officer. De compliance officer deelt onverwijld aan de betrokken

verbonden persoon mee of hij als insider wordt aangemerkt, en stelt hem op de hoogte van de gevolgen van de aanwijzing als insider.

- 4.2.6 Iedere verbonden persoon is desgevraagd gehouden alle informatie aan de compliance officer te verschaffen in het kader van de strikte naleving van de gedragscode.

Hoofdstuk 5 Algemene uitgangspunten persoonlijke transacties (insiderregeling)

- 5.1 Er mag nooit een verband bestaan tussen de transacties in financiële instrumenten die het pensioenfonds tot stand brengt of doet komen en een persoonlijke transactie van de insider of een gelieerde derde.
- 5.2 De insider dient zich te onthouden van elk handelen of de redelijkerwijs voorzienbare schijn daarvan, met gebruik van voorwetenschap of met anderszins vertrouwelijke informatie. Hij dient voorts iedere vermenging van zakelijke en privébelangen respectievelijk de redelijkerwijs voorzienbare schijn daarvan, te vermijden.
- 5.3 Het is een insider die beschikt over voorwetenschap niet toegestaan:
- deze informatie aan een derde mee te delen, anders dan in de normale uitoefening van zijn functie binnen het pensioenfonds, of
 - een derde aan te bevelen of ertoe aan te zetten transacties te verrichten of te bewerkstelligen in die financiële instrumenten, waarop de voorwetenschap betrekking heeft.
- Het vorige is van overeenkomstige toepassing op een insider die weet of redelijkerwijs moet vermoeden dat hij over voorwetenschap beschikt.
- 5.4 De insider onthoudt zich van het binnen 24 uur opdracht te geven tot zowel een aan- als verkooporder voor transacties in een financieel instrument van dezelfde uitgevende instelling, rechtspersoon of vennootschap.
- 5.5 Als niet (meer) wordt belegd in financiële instrumenten door de insider en/of door degene waarvoor de insider gemachtigd is privétransacties te verrichten of te bewerkstelligen, dan dient de insider deze informatie ook door te geven.
- 5.6 Iedere verbonden persoon die als insider wordt aangemerkt wordt daarvan onverwijld door de compliance officer op de hoogte gebracht. De betreffende verbonden persoon wordt tevens geïnformeerd over de gevolgen van de aanwijzing als insider. De insider wordt verder in kennis gesteld van de procedures en maatregelen gericht op het toezicht op de persoonlijke transacties.

Hoofdstuk 6 Toezicht op persoonlijke transacties (insiderregeling)

- 6.1 De compliance officer houdt gegevens bij van de gemelde of door hem onderkende persoonlijke transacties en vermeldt daarbij in voorkomend geval tevens of de desbetreffende transactie goedgekeurd of verboden is.
- 6.2 De insider onderschrijft dat de compliance officer bevoegd is een onderzoek in te (doen) stellen naar enige beleggingstransactie verricht door, in opdracht van of ten behoeve van de insider. De insider is verplicht jaarlijks te bevestigen aan de compliance officer dat hij de uitgangspunten van de insiderregeling onderschrijft en heeft nageleefd.
- 6.3 De insider is in het kader van een strikte naleving van de gedragscode gehouden desgevraagd alle informatie over een door hem of voor hem verrichte persoonlijke transactie aan de compliance officer te verstrekken.
- 6.4 De insider is verplicht desgevraagd opdracht te geven aan het pensioenfonds, een andere instelling, lasthebber, beleggingsinstelling of andere derde, om de compliance officer alle informatie te verstrekken over enige voor hem of in zijn opdracht verrichte persoonlijke transactie.
- 6.5 De compliance officer is bevoegd over de uitkomst van dit onderzoek schriftelijk te rapporteren aan de voorzitter van het bestuur. Alvorens de compliance officer daarover rapporteert, wordt de insider in de gelegenheid gesteld om te reageren op de bevindingen van het onderzoek. De insider wordt door de voorzitter van het bestuur van de definitieve uitkomst van het onderzoek in kennis gesteld.
- 6.6 Van het toezicht op de persoonlijke transacties van de insider zijn vrijgesteld:
- transacties in obligaties uitgegeven door de Staat en andere overheden,
 - transacties in financiële instrumenten waarvan het beheer, op grond van een schriftelijke overeenkomst is overgedragen aan een professionele vermogensbeheerder, op zodanige voorwaarden dat de insider geen invloed kan uitoefenen op de fondsselectie of op afzonderlijke transacties,
 - transacties in indexfondsen of in ter beurse genoteerde rechten van deelneming in (semi)open-ended-beleggingsinstellingen, mits de insider binnen die instelling geen functie vervult.

Desgewenst overlegt de insider aan de compliance officer de overeenkomst die ten grondslag ligt aan de overdracht van het beheer van zijn vermogensbestanddelen.

Hoofdstuk 7 Vertrouwelijkheid

De Verbonden Persoon mag geen informatie over zaken – inclusief individuele pensioengegevens en beleggingen – van het pensioenfonds, waarvan hij weet of redelijkerwijs behoort te weten dat die informatie vertrouwelijk is, aan derden bekend maken of ten eigen voordele of ten behoeve van anderen dan het pensioenfonds gebruiken.

Hoofdstuk 8 Meldingsplicht

- 8.1 Iedere verbonden persoon is verplicht elk (potentieel) tegenstrijdig belang, integriteitsrisico of reputatierisico te melden aan de compliance officer. Pogingen van een (aspirant)relatie tot beïnvloeding dienen eveneens onmiddellijk te worden gemeld.
- 8.2 De insider is verplicht om onverwijld persoonlijke transacties aan de compliance officer te melden.

Hoofdstuk 9 Compliance officer

- 9.1 Het pensioenfonds wijst een compliance officer aan. De compliance officer vervult een onafhankelijke rol binnen het pensioenfonds. De compliance officer wordt benoemd door het bestuur van het pensioenfonds. De compliance officer rapporteert aan de voorzitter van het bestuur, zowel voor de dagelijkse gang van zaken, als in het geval zich een bijzondere omstandigheid heeft voorgedaan.
- 9.2 Het pensioenfondsbestuur legt de taken van de compliance officer schriftelijk vast. Het bestuur waarborgt dat de compliance officer over voldoende bevoegdheden beschikt voor het uitoefenen van toezicht op de naleving van relevante wettelijke bepalingen en de gedragscode en diens onafhankelijke positie ten opzichte van degenen die zijn onderworpen aan zijn toezicht. De compliance officer houdt toezicht op de deugdelijkheid en effectiviteit van interne regels en procedures. Hij rapporteert ten minste jaarlijks over zijn werkzaamheden en doet aanbevelingen op basis van de resultaten van zijn werkzaamheden. Het intern toezicht ziet toe op de in het kader van de naleving van de gedragscode door de compliance officer uitgevoerde werkzaamheden.
- 9.3 Het bestuur legt vast welke acties zijn ondernomen naar aanleiding van de bevindingen van de compliance officer.

- 9.4 Indien de compliance officer daartoe aanleiding ziet, kan hij verbonden personen verplichten op eerste verzoek alle informatie te (laten) verstrekken omtrent enige door of ten behoeve van hen verrichte persoonlijke transacties. De compliance officer controleert of die transacties aan de toepasselijke regels, voorschriften en aanwijzingen voldoen.
- 9.5 De compliance officer adviseert en informeert, gevraagd én ongevraagd, verbonden personen over de uitleg en toepassing van de gedragscode.
- 9.6 De compliance officer documenteert zijn werkmethoden en werkzaamheden en administreert en archiveert alle informatie die hem door verbonden personen (de meldingen van persoonlijke transacties inbegrepen) of derden is verstrekt. Hij bewaart afschriften van alle overeenkomsten en de jaarlijkse verklaringen die verbonden personen hem moeten verstrekken. Tevens administreert en archiveert de compliance officer alle door hem verrichte controles, onderzoeken en de genomen acties, alsmede overige van belang zijnde informatie, memoranda en correspondentie. De gegevens worden ten minste zeven jaar bewaard.
- 9.7 De compliance officer legt een lijst aan van alle verbonden personen die als insider worden aangemerkt. De compliance officer deelt onverwijld aan de op de lijst opgenomen verbonden personen mee dat zij als insider zijn aangemerkt en hij stelt hen op de hoogte van de gevolgen van de aanwijzing als insider.
- 9.8 De compliance officer en de voorzitter van het bestuur zijn gehouden tot geheimhouding van de informatie, die is verstrekt door verbonden personen of derden. De geheimhouding kan worden doorbroken in het geval de goede uitoefening van hun functie daartoe noodzaakt.

Hoofdstuk 10 Ondertekening gedragscode en jaarlijkse verklaring

- 10.1 Iedere verbonden persoon moet bij aanvang van zijn functie bij het pensioenfonds de gedragscode ondertekenen, waarmee hij zich verbindt alle voor hem relevante regels uit deze gedragscode na te leven.
- 10.2 Aan het eind van ieder kalenderjaar of bij het niet langer verbonden zijn aan het pensioenfonds, moet iedere verbonden persoon een verklaring ondertekenen over de juiste naleving van de geldende bepalingen in de gedragscode over het afgelopen jaar. Bij het niet langer verbonden zijn aan het pensioenfonds blijven de uit de gedragscode geldende normen

van toepassing op de verbonden persoon, voor zover dat uit hun aard voortvloeit.

Hoofdstuk 11 Sancties

Het handelen door de verbonden persoon in strijd met de gedragscode wordt beschouwd als een ernstige inbreuk op het vertrouwen dat het pensioenfonds als werkgever of anderszins in de verbonden persoon moet kunnen stellen. Een dergelijk handelen kan reden zijn tot het opleggen van een sanctie, waaronder – afhankelijk van de ernst van de overtreding en afhankelijk van de aard van de relatie tussen verbonden persoon en pensioenfonds – een waarschuwing, het ongedaan maken van het door de verbonden persoon behaalde voordeel, overplaatsing, schorsing, of andere disciplinaire of arbeidsrechtelijke maatregel, ontslag op staande voet niet uitgezonderd. Een overtreding kan worden gemeld aan de toezichthouder(s) en – indien van toepassing – bij het Dutch Securities Institute. Het voorgaande laat onverlet een vordering tot schadevergoeding en/of aangifte bij de justitiële autoriteiten.

Hoofdstuk 12 Advies en bezwaar

Indien de verbonden persoon twijfelt over de uitleg van de op hem van toepassing zijnde gedragsregels, is hij verplicht het advies van de compliance officer in te winnen. De compliance officer is bevoegd een voor de verbonden persoon bindend advies te doen. Tegen het advies van de compliance officer kan de verbonden persoon bezwaar maken bij de voorzitter van het bestuur of een aangewezen beroepsorgaan. Het maken van bezwaar heeft geen schorsende werking ten aanzien van de uitspraak van de compliance officer.

Hoofdstuk 13 Onvoorziene omstandigheden

Voor kwesties waarin deze gedragscode niet voorziet, beslist de voorzitter van het bestuur. Indien de kwestie de voorzitter van het bestuur betreft, dan beslist de vicevoorzitter en/of de compliance officer.

Hoofdstuk 14 Slotbepalingen

- 14.1 Het bestuur kan de gedragscode te allen tijde wijzigen.
- 14.2 De onderhavige gedragscode vervangt met ingang van 12 februari 2021 alle vorige gedragscodes.

Bijlage 3 Incidentenregeling Stichting Pensioenfonds Thales Nederland

{OPEN}

Incidentenregeling Stichting Pensioenfonds Thales Nederland

Datum: 29-11-2024
Versie: 1.0

Inhoudsopgave

1	Inleiding.....	3
1.1	Wettelijk kader	3
1.2	Reikwijdte Incidentenregeling	3
1.3	Samenhangende interne regelingen	3
2	Definities	4
3	Governance	6
4	Behandeling van incidenten	6
4.1	Melden van Incidenten	6
4.2	Beoordeling van Incidenten	6
4.2.1	Beoordeling van Operationele-, Integriteits- en Overige Incidenten	6
4.2.2	Beoordeling van ICT-gerelateerde Incidenten	7
4.3	Behandeling van Incidenten	7
4.4	Afronding van Incidenten	8
4.5	Spoedeisend belang	9
4.6	Melden toezichthouder en overige communicatie	9
4.6.1	Meldingen van Operationele-, Integriteits- en Overige Incidenten	9
4.6.2	Meldingen van significante ICT-gerelateerde Incidenten	9
4.6.3	Vrijwillige melding van significante Cyberdreigingen	10
4.6.4	Informereren van deelnemers over significante ICT-gerelateerde Incidenten	10
4.6.5	Rapporteren raming kosten en verliezen significante ICT-gerelateerde Incidenten	10
5	Vastlegging van Incidenten	10
5.1	Vastlegging in Incidentenregister	10
5.2	Vastlegging in Incidentendossier en waarborging vertrouwelijkheid	11
6	Rapportage	11
6.1	Voortgangsrapportages afhandeling Incidenten	11
6.2	Periodieke Incidentenrapportages aan Bestuur	11
6.3	Post-incidentevaluatie ICT-gerelateerde Incidenten	11
7	Omgang met meldingen	12
8	Inwerkingtreding	12
	Bijlage 1 - Classificatiecriteria en materialiteitsdrempels significante ICT-gerelateerde Incidenten en cyberdreigingen	13

1 Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van Stichting Pensioenfonds Thales Nederland (hierna: het Fonds).

Deze Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een Incident binnen het Fonds. Doel van deze regeling is het voorkomen van schade aan de beheerste en integere bedrijfsvoering en goede naam van het Fonds, alsmede het beperken van mogelijke gevolgschade.

Daarnaast wil het Fonds leren van Incidenten om herhaling te voorkomen. Het Fonds streeft er naar een betrouwbare, transparante en lerende organisatie te zijn. Daarbij past een cultuur waarin medewerkers Incidenten kunnen melden en waarin helder is hoe met deze melding zal worden omgegaan.

1.1 Wettelijk kader

Met deze regeling geeft het Fonds uitvoering aan de vereisten van de Pensioenwet, de Algemene Verordening Gegevensbescherming (AVG), de Verordening betreffende digitale operationele weerbaarheid voor de financiële sector (DORA) en de Code Pensioenfondsen, inzake de omgang met en vastlegging van Incidenten.

1.2 Reikwijdte Incidentenregeling

De Incidentenregeling is van toepassing op alle verbonden personen. Van Uitbestedingsrelaties en externe (ICT)dienstverleners van het Fonds wordt verwacht dat zij beschikken over een eigen Incidentenregeling die voldoet aan de eisen vanuit de regeling van het Fonds.

1.3 Samenhangende interne regelingen

Er bestaan binnen het Fonds verschillende regelingen, processen en procedures (bijvoorbeeld de Gedragscode, de Klokkenluidersregeling en de Regeling ongewenst gedrag op het werk). Ook in deze regelingen zijn gedragsnormen opgenomen. Deze conflicteren niet met de Incidentenregeling en zijn eveneens van toepassing.

De samenhang tussen de verschillende regelingen is als volgt:

- Iedere Verbonden Persoon die een (vermoeden van een) Incident constateert is gehouden dit te melden aan de Manager Pensioenfonds.
- Indien het belang van de onderneming, van derden of de bescherming van de eigen positie van de Verbonden persoon dit vraagt (bijvoorbeeld omdat hij vreest dat een melding nadelige gevolgen kan hebben voor zijn positie of indien aan een eerdere melding geen gevolg is gegeven), wordt het incident door de Verbonden persoon gemeld bij de Compliance Officer als Misstand conform de Klokkenluidersregeling. Het oordeel van de Verbonden persoon dat een melding dient plaats te vinden conform de Klokkenluidersregeling is daarbij doorslaggevend.
- Ongewenste gedragingen van een andere Verbonden persoon kunnen worden gemeld als Klacht bij de Vertrouwenspersoon conform de Regeling ongewenst gedrag op het werk.

2 Definities

Toezichthouder:

De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) het Fonds.

Incident:

Een gebeurtenis die een (ernstig) gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het Fonds, en/of een gebeurtenis waarbij directe of indirecte (financiële) schade ontstaat door ontoereikende of falende interne processen, Verbonden personen of systemen of door externe gebeurtenissen, dan wel een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming (AVG).

Onder incidenten worden in ieder geval verstaan:

- een (dreigende) bewuste schending van wet- en regelgeving;
- een (dreiging van) bewust onjuist informeren van publieke organen;
- een (dreigende) schending van binnen het Fonds geldende gedragsregels;
- (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie over deze feiten;
- een ernstig gevaar voor de integere bedrijfsuitoefening van het Fonds;
- gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media;
- fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in de hoedanigheid van Verbonden persoon;
- een (mogelijk) aanwijzing van een Toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;
- overige strafbare feiten.

Er wordt een onderscheid gemaakt tussen Integriteitsincidenten, ICT-gerelateerde Incidenten, Operationele Incidenten en Overige Incidenten.

Integriteitsincident:

Een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende organisatie.

ICT-gerelateerd Incident:

Een gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door het Fonds zijn gepland en die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of op de door het Fonds verleende diensten. Deze ICT-gerelateerde incidenten kennen ook de volgende subcategorieën:

- **Ernstig ICT-gerelateerd incident:** Een ICT-gerelateerd Incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van het Fonds ondersteunen;
- **Cyberdreiging:** Elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden;

- **Significante Cyberdreiging:** Een cyberdreiging waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ernstig ICT-gerelateerd Incident of een ernstig betalingsgerelateerd operationeel of beveiligingsincident.
- **Cyberaanval:** Een kwaadwillig ICT-gerelateerd Incident dat het gevolg is van een door een dreigingsactor gepleegde poging om een actief te vernietigen, bloot te stellen, te veranderen, buiten werking te stellen, te stelen of er ongeoorloofde toegang toe te verkrijgen of er ongeoorloofd gebruik van te maken.

Operationeel Incident:

Een Operationeel Incident is een gebeurtenis die plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het Fonds en waarbij er een inbreuk is geweest op de bedrijfsvoering.

Overige Incidenten:

Alle Incidenten, die niet beschouwd kunnen worden als Integriteitsincidenten, ICT-gerelateerde Incidenten of Operationele Incidenten.

Crisismanagementteam:

Het Crisismanagementteam wordt bijeengeroepen wanneer een ICT-gerelateerd incident leidt tot een crisissituatie, in lijn met het ICT-crisiscommunicatieprotocol van het Fonds. Het crisismanagementteam bestaat tenminste uit de Manager Pensioenfonds, het Dagelijks Bestuur en de Communicatiecommissie.

Compliance Officer:

Degene die verantwoordelijk is voor het uitvoeren van de compliancewerkzaamheden.
Mevrouw S. Holwerda, arbeidsjuriste.

Verbonden Personen:

- leden van het bestuur,
- leden van de Raad van Toezicht en het Verantwoordingsorgaan;
- externe leden van commissies die zijn ingesteld ter ondersteuning van het bestuur,
- medewerkers van het bestuursbureau, waaronder mensen die tijdelijk werken/inhuur,
- andere (groepen van) personen die door het bestuur worden aangewezen,
- sleutelfunctiehouders en de vervullers van de sleutelfuncties.

Uitbestedingsrelatie:

Een partij waaraan het Fonds werkzaamheden heeft uitbesteed.

Derde aanbieder van ICT-diensten (ICT-dienstverlener):

Een onderneming die ICT-diensten verleent aan het Fonds conform de definitie van DORA¹.

¹ "ICT-diensten" zijn digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten.

3 Governance

Incidenten worden over het algemeen gemeld door een verbonden persoon, een uitbestedingsrelatie of een externe (ICT-)dienstverlener.

Het Fonds draagt er zorg voor dat de verbonden personen, uitbestedingsrelaties en externe (ICT-) dienstverleners bekend zijn met deze Incidentenregeling en weten bij wie een Incident gemeld moet worden.

De beoordeling, classificatie, toewijzing en monitoring van de behandeling en afhandeling van Incidenten vindt plaats door de eerste lijn. Meldingen komen in eerste instantie binnen bij de Manager Pensioenfonds. Als sprake is van een crisissituatie voortvloeiend uit een ICT-gerelateerd incident, wordt het Crisismanagementteam bijeengeroepen.

Het bestuur van het Fonds is te allen tijde eindverantwoordelijk voor de adequate afhandeling van Incidenten.

4 Behandeling van incidenten

4.1 Melden van Incidenten

Iedere Verbonden persoon die een (vermoeden van een) Incident constateert is gehouden dit te melden aan de Manager Pensioenfonds. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem gedaan worden.

Als zich bij een partij waaraan het Fonds werkzaamheden heeft uitbesteed een Incident voordoet, meldt deze Uitbestedingsrelatie het Incident aan de Manager Pensioenfonds. Het Fonds draagt er zorg voor dat de Uitbestedingsrelatie bekend is met deze regeling en weet bij wie een Incident gemeld moet worden.

Het staat een Verbonden persoon vrij een (een vermoeden van een) Incident ook aan de Compliance Officer te melden. Deze is gehouden de Manager Pensioenfonds op de hoogte te brengen.

4.2 Beoordeling van Incidenten

De Manager Pensioenfonds beoordeelt de melding en bepaalt of er sprake is van een Incident en zo ja, of er dan sprake is van een Operationeel Incident, ICT-gerelateerd Incident, Integriteitsincident of een Overig Incident. Dit oordeel wordt vastgelegd in het Incidentenregister.

De Manager Pensioenfonds brengt de melder van zijn beoordeling op de hoogte. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

4.2.1 Beoordeling van Operationele-, Integriteits- en Overige Incidenten

De Manager Pensioenfonds bepaalt of het Operationele-, Integriteits- of Overige Incident kwalificeert als een Significant Incident. Een Incident kwalificeert zich als Significant Incident als er sprake is van een Incident dat een ernstig gevaar vormt voor de beheerste en integere bedrijfsvoering.

Hiervan is in ieder geval sprake als:

- aangifte is of wordt gedaan bij justitiële autoriteiten;
- het voortbestaan van het Fonds wordt bedreigd of zou kunnen worden bedreigd;
- er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere bedrijfsvoering door het Fonds;
- mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het Fonds;
- of de ernst, de omvang of de overige omstandigheden van het Incident in aanmerking genomen, de Toezichthouder in verband met haar toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.

4.2.2 Beoordeling van ICT-gerelateerde Incidenten

De Manager Pensioenfonds bepaalt aan de hand van de classificatiecriteria en respectievelijke materialiteitsdrempels zoals opgenomen in Bijlage 1 of het ICT-gerelateerde Incident een 'Significant' ICT-gerelateerd Incident of 'Significante' Cyberdreiging betreft.

Om vast te stellen of het een Significant ICT-gerelateerd Incident betreft, worden door de Manager Pensioenfonds tenminste de volgende classificatiecriteria beoordeeld:

- a. Cliënten, financiële tegenpartijen en transacties;
- b. Reputatieschade;
- c. Duur en uitvaltijd van de dienst;
- d. Geografische spreiding;
- e. Gegevensverliezen;
- f. Mate waarin getroffen diensten als cruciaal kunnen worden aangemerkt; en
- g. Economische gevolgen.

De beoordeling aan de hand van deze classificatiecriteria vindt plaats op basis van materialiteitsdrempels. Deze drempels bepalen de grens of een ICT-gerelateerd Incident als 'Significant' wordt geclassificeerd. Verder geldt dat als een ICT-gerelateerd Incident voor meerdere categorieën gezamenlijk boven een materialiteitsgrens komt, het Incident ook als 'Significant' wordt geclassificeerd.

Om vast te stellen of een Cyberdreiging een Significante Cyberdreiging betreft, toetst de Manager Pensioenfonds bovendien aan de uitputtende lijst van materialiteitsdrempels zoals opgenomen in Bijlage 1.

Als sprake is van een ICT-gerelateerd Incident bij kritieke/belangrijke systemen, dan is er altijd sprake van classificatie 'Significant'.

4.3 Behandeling van Incidenten

4.3.1 Behandeling van Operationele-, Integriteits- en Overige Incidenten

Indien de Manager Pensioenfonds van mening is dat er sprake is van een Operationeel-, Integriteits- of Overige Incident, dan brengt deze het Bestuur op de hoogte. Indien dit een mogelijk Integriteitsincident of een Overig Incident betreft, dan brengt de Manager Pensioenfonds in overleg met het Bestuur eventueel ook de Compliance Officer op de hoogte.

Door het Bestuur wordt, na advies van de Manager Pensioenfonds, besloten of en wanneer andere organen van het Fonds, sleutelfunctiehouders en/of overige belanghebbenden op de hoogte worden gebracht van het Incident.

De Manager Pensioenfonds zorgt voor de afhandeling van het Incident. Hieronder ook de Integriteitsincidenten en Overige Incidenten, tenzij het Bestuur, na advies van de Manager Pensioenfonds, besluit dat, gelet op de aard of achtergronden van het incident, afwikkeling door een andere functionaris of een speciaal daarvoor te benoemen Onderzoekscommissie de voorkeur geniet. Een Onderzoekscommissie kan bestaan uit medewerkers van het Fonds en/of externe deskundigen.

Als een onderzoek wordt verricht door een andere persoon dan de Manager Pensioenfonds of door een Onderzoekscommissie is/zijn de onderzoeker(s) gehouden de Manager Pensioenfonds op de hoogte te brengen en te houden van alle ontwikkelingen in het onderzoek vanwege haar coördinerende en registrerende rol. Als de Manager Pensioenfonds zelf onderwerp van onderzoek is, zal de Voorzitter van het Bestuur de taken van de Manager Pensioenfonds rondom de afhandeling van het incident op zich nemen.

De Manager Pensioenfonds bewaakt de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties en rapporteert hierover aan het Bestuur.

4.3.2 Behandeling van ICT-gerelateerde Incidenten

Indien de Manager Pensioenfonds van mening is dat er sprake is van een ICT-gerelateerd Incident, dan brengt deze het Bestuur op de hoogte. Als uit de beoordeling is gebleken dat het een significant ICT-gerelateerd incident betreft, dan wordt bovendien het Crisismanagementteam bijeengeroepen, in lijn met het ICT-crisiscommunicatieprotocol van het Fonds.

Het Crisismanagementteam is vervolgens verantwoordelijk voor de behandeling van het incident in lijn met deze Incidentenregeling en het ICT-crisiscommunicatieprotocol.

4.4 Afronding van Incidenten

Na de behandeling van elk Incident wordt, ter afronding, door het Fonds besloten of er maatregelen genomen dienen te worden.

De genomen maatregelen zullen zijn gebaseerd op de aard van het Incident en de daaruit voortvloeiende gevolgen. De maatregelen zullen onder meer zijn gericht op het beheersen en beperken van het optredende risico, het bevestigen van geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – voortvloeiend uit het Incident om herhaling in de toekomst te voorkomen.

De eindverantwoordelijkheid voor de afronding van het Incident en de eventuele getroffen maatregelen ligt bij het Bestuur.

4.5 Spoedeisend belang

Indien de aard van het Incident snel handelen vereist, is de Voorzitter van het Bestuur, of diens plaatsvervanger, bevoegd om namens het Bestuur een (voorlopig) besluit te nemen over de afhandeling van het Incident.

De Voorzitter van het Bestuur is gehouden om de overige leden van het Bestuur zo snel mogelijk op de hoogte te brengen van verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het Bestuur voor te leggen.

4.6 Melden toezichthouder en overige communicatie

Het Bestuur van het Fonds beslist over de communicatie, zowel intern als extern, met betrekking tot Incidenten.

4.6.1 Meldingen van Operationele-, Integriteits- en Overige Incidenten

Het bestuur raadpleegt de Manager Pensioenfonds en de sleutelfunctiehouder Risicobeheer en informeert onverwijld de toezichthouder wanneer het Operationele-, Integriteits- of Overige Incident een Significant Incident betreft, zoals vastgesteld tijdens de beoordeling (zie hoofdstuk 'Beoordeling van Incidenten').

De informatie die aan de toezichthouder wordt verstrekt, omvat in elk geval:

- a. de feiten en omstandigheden van het Incident;
- b. informatie over de functie, hoedanigheid en positie van degene of degenen die het Incident heeft of hebben bewerkstelligd;
- c. de maatregelen die naar aanleiding van het Incident zijn genomen.

4.6.2 Meldingen van significante ICT-gerelateerde Incidenten

Als een significant ICT-gerelateerde Incident wordt geconstateerd, moet het Fonds een initieel, een tussen- en finaal Incidentrapport indienen bij DNB. De rapportages volgen een onder DORA voorgeschreven format.

De Manager Pensioenfonds en het Crisismanagementteam zijn verantwoordelijk voor het opstellen van de rapportages en, na goedkeuring door de het Bestuur, het indienen van de rapportages bij DNB.

Daarbij borgt het Fonds dat deze verschillende rapportages tijdig aan DNB worden verstrekt, binnen de hieronder beschreven deadlines:

- a. Het initiële rapport moet worden ingediend binnen 4 uur, maar uiterlijk binnen 24 uur nadat is vastgesteld dat het Incident significant is;
- b. Het tussenrapport moet worden ingediend binnen 72 uur na indiening van het initieel rapport;
- c. Het finale rapport moet worden ingediend binnen een maand na indiening van het tussenrapport.

Het Fonds kan de rapportageverplichtingen rondom ICT-gerelateerde Incidenten uitbesteden. Als het Fonds hiervoor kiest, borgt het Fonds dat de verantwoordelijkheden, rechten en plichten van de ICT-dienstverlener adequaat zijn vastgelegd. Hierbij worden tenminste de volgende elementen behandeld:

- a. aanmelding uitbesteding bij DNB;
- b. controle van de door de ICT-dienstverlener opgestelde melding voorafgaand aan verzending; en
- c. informatievoorziening rondom de communicatie tussen de ICT-dienstverlener en DNB.

4.6.3 Vrijwillige melding van significante Cyberdreigingen

DORA stelt dat het Fonds significante Cyberdreigingen op vrijwillige basis kan melden aan de Toezichthouder wanneer zij van oordeel is dat de dreiging relevant is voor het financiële stelsel, de gebruikers van diensten of de cliënten. Het Fonds heeft ervoor gekozen dergelijke vrijwillige meldingen niet te doen.

Het bestuur heeft de mogelijkheid om informatie en inlichtingen over cyberdreigingen uit te wisselen met andere pensioenfondsen. De informatie die uitgewisseld wordt, is bedoeld om de digitale operationele weerbaarheid te versterken.

4.6.4 Informeren van deelnemers over significante ICT-gerelateerde Incidenten

Het Fonds zal ook deelnemers onverwijld en adequaat informeren over significante ICT-gerelateerde Incidenten die gevolgen hebben voor de financiële belangen van deelnemers. De kennisgeving moet inzicht geven in zowel (de aanleiding van) het Incident als de getroffen maatregelen om de gevolgen te beperken en herhaling te voorkomen. Het proces van kennisgeving, inclusief de verantwoordelijke binnen het Fonds voor de coördinatie van de communicatie, is vastgelegd in het ICT-crisiscommunicatieprotocol van het Fonds. Het ICT-crisiscommunicatieprotocol betreft een losstaand document.

4.6.5 Rapporteren raming kosten en verliezen significante ICT-gerelateerde Incidenten

Indien DNB dit verzoekt, verstrekt het Fonds aan DNB een raming van de individuele en geaggregeerde kosten en verliezen als gevolg van significante ICT-gerelateerde Incidenten. Deze raming volgt uit de berekening van de economische gevolgen die het Fonds uitvoert om bepalen of een ICT-gerelateerd Incident een significant Incident betreft. Rapporteren richting DNB gebeurt via een gestandaardiseerd template kostenraming.

5 Vastlegging van Incidenten

5.1 Vastlegging in Incidentenregister

Meldingen van Incidenten en de (uitkomst van de) beoordeling door de Manager Pensioenfonds van het Incident worden geregistreerd in het Incidentenregister, tenzij de gevoeligheid van de informatie een dergelijke registratie in de weg staat. Gedurende het verdere proces worden in het dossier de naar het oordeel van de Manager Pensioenfonds relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel (extern uitgevoerd) onderzoek.

In het Incidentenregister maakt het Fonds een onderscheid tussen het type Incident en tussen de impact en urgentie van een Incident. Indien het Incident een significant ICT-gerelateerd Incident betreft, neemt de Manager Pensioenfonds in het Incidentenregister de aanvullende informatie op zoals voorgeschreven onder DORA.

5.2 Vastlegging in Incidentendossier en waarborging vertrouwelijkheid

Gedurende het hele proces worden in het dossier relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek.

Deze Incidentendossiers worden in een beveiligde omgeving bewaard zodat de vertrouwelijkheid wordt gewaarborgd. Als sprake is van de betrokkenheid van een Verbonden persoon, worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen de Manager Pensioenfonds en de Voorzitter van het Bestuur toegang hebben tot deze gegevens.

De melding en de daarbij beschikbaar gestelde gegevens worden door alle betrokken partijen strikt vertrouwelijk behandeld. De identiteit van de melder wordt niet opgenomen in communicatie naar derden, tenzij daar een wettelijke verplichting toe bestaat.

Eenieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident betracht daarover uiterste geheimhouding, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen. Indien voor de afronding van het Incident openheid van zaken is vereist, kan het bestuur beslissen dat de verplichting tot geheimhouding geheel of gedeeltelijk vervalt.

6 Rapportage

6.1 Voortgangsrapportages afhandeling Incidenten

De voortgang van de afhandeling van Incidenten wordt in de vergadering van het Bestuur geagendeerd. Het Bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het Bestuur kan de Manager Pensioenfonds toezien op de daadwerkelijke opvolging.

Als het Incident zich heeft voorgedaan bij en wordt behandeld door een van de Uitbestedingsrelaties van het Fonds, dan borgt het bestuur dat zij tijdige en volledige (tussentijdse) rapportages ontvangt die het bestuur in staat stelt te monitoren op de adequate afhandeling van het Incident door de Uitbestedingsrelatie.

6.2 Periodieke Incidentenrapportages aan Bestuur

In de rapportage(s) zoals die periodiek aan het Bestuur worden aangeboden, wordt inzicht gegeven in het aantal en de classificatie van Incidenten dat zich de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de afhandeling van Incidenten en de naar aanleiding van deze Incidenten genomen maatregelen.

6.3 Post-incidentevaluatie ICT-gerelateerde Incidenten

In het geval van ICT-gerelateerde Incidenten (waaronder Cyberaanvallen) wordt tijdens de post-Incidentevaluatie door het Fonds specifiek stilgestaan bij:

- a. De snelheid waarmee is gereageerd op veiligheidswaarschuwingen en de effecten en de ernst van ICT-gerelateerde Incidenten zijn vastgesteld;
- b. De kwaliteit en snelheid bij het verrichten van een forensische analyse, als deze passend wordt geacht;

- c. De doeltreffendheid van Incidentescalatie binnen het Fonds;
- d. De doeltreffendheid van interne en externe communicatie.

7 Omgang met meldingen

Het Fonds gaat er altijd vanuit dat een melding van een Incident te goeder trouw is gedaan, tot het moment dat zij overtuigd is geraakt van het tegendeel.

Het Fonds draagt er zorg voor dat een melder, ongeacht de wijze waarop deze melding heeft gemaakt van een Incident, op geen enkele wijze in zijn/haar/hen positie bij het Fonds benadeeld wordt, voor zover te goeder trouw gehandeld is.

Het Fonds draagt er zorg voor dat niemand wordt benadeeld in zijn/ haar/hen positie bij het Fonds, vanwege het uitoefenen van de taken en/of verplichtingen uit deze regeling.

In geval van intrekking van een melding zal het Fonds, ongeacht de wijze waarop melding is gemaakt van een Incident, zich ervan vergewissen dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

Een Verbonden persoon die willens en wetens heeft deelgenomen aan of veroorzaker is van een Incident, zal bij melding van dit Incident geen recht kunnen ontlenen aan de beschermingsregels zoals die gelden voor een te goeder trouw handelende Verbonden persoon.

8 Inwerkingtreding

Deze Incidentenregeling treedt in werking op 29-11-2024 en vervangt de vorige versie van 09-11-2018.

Bijlage 1 - Classificatiecriteria en materialiteitsdrempels significante ICT-gerelateerde Incidenten en cyberdreigingen

Onderstaande tabel is afgeleid van de specifieke DORA Level 2 vereisten. Het Fonds zal de hierin opgenomen materialiteitsdrempels zo goed mogelijk toepassen bij de beoordeling van ICT-gerelateerde incidenten.

Classificatie categorieën	Classificatie criteria	Materialiteitsdrempels significante Incidenten	Materialiteitsdrempels significante Cyberdreiging
Cliënten, financiële tegenpartijen en transacties	Aantal cliënten	Aantal cliënten > 10 %	Een cyberdreiging wordt als significant beschouwd wanneer aan alle voorwaarden is voldaan: - de Cyberdreiging kan gevolgen hebben of zou gevolgen kunnen hebben voor kritieke of belangrijke functies van het Fonds, of voor andere financiële entiteiten, derde aanbieders, cliënten of financiële tegenpartijen, op basis van informatie waarover het Fonds beschikt; - de Cyberdreiging heeft een grote kans om werkelijkheid te worden bij het Fonds of bij andere financiële entiteiten, rekening houdend met ten
	Aantal financiële tegenpartijen dat een overeenkomst heeft met het Fonds	Aantal cliënten > 100 000 Aantal financiële tegenpartijen > 30 %	
	Hoeveelheid of aantal transacties waarbij een geldbedrag betrokken is waarbij ten minste één deel van de transactie in de EU wordt uitgevoerd	Aantal transacties > 10 % het gemiddelde dagelijkse aantal uitgevoerde transacties Aantal transacties > 10 % de dagelijkse gemiddelde waarde van de uitgevoerde transacties	
		Cliënten of financiële tegenpartijen als relevant zijn aangemerkt	
Reputatieschade	Tenminste (één) van de volgende criteria: 1. Er is over het Incident bericht in de media; 2. Het Incident heeft geleid tot herhaalde klachten van verschillende cliënten of financiële tegenpartijen over diensten of kritieke zakelijke relaties	De materialiteitsdrempel wordt bereikt wanneer aan één van criteria voor Reputatieschade is voldaan.	
	3. het Fonds zal als gevolg van het Incident niet in staat zijn om aan de wettelijke vereisten te voldoen; 4. Verlies van cliënten of financiële tegenpartijen. De mate van zichtbaarheid die het Incident heeft of wellicht zal hebben met betrekking tot elk in de benoemde criteria.		
Duur en uitvaltijd van de dienst	Metten duur van Incident vanaf:	Duur van Incident => 24 uur	

	- Het moment waarop het Incident zich voordoet tot het moment het is opgelost; of - Het moment het Incident is ontdekt; of - Het moment waarop het Incident is geregistreerd in netwerk- of systeemlogbestanden of andere gegevensbronnen.		minste de volgende elementen: - o toepasselijke risico's in verband met de cyberdreiging op kritieke of belangrijke functies, met inbegrip van potentiële kwetsbaarheden van de systemen van de financiële entiteit die kunnen worden uitgebuit; - o de capaciteiten en intentie van dreigingsactoren voor zover bekend bij het Fonds; - o de aanhoudende dreiging en alle verworven kennis over Incidenten die gevolgen hebben gehad voor de financiële entiteit of haar derde aanbieder, cliënten of financiële tegenpartijen; - de Cyberdreiging kan aan een van de volgende situaties voldoen:
	De uitvaltijd van de dienst meten vanaf het moment dat de dienst geheel of gedeeltelijk niet beschikbaar is voor cliënten, financiële tegenpartijen of andere interne of externe gebruikers tot het moment waarop de reguliere activiteiten of verrichtingen zijn hersteld tot het niveau van dienstverlening dat vóór het Incident werd verleend De uitvaltijd van de dienst veroorzaakt vertraging nadat de geregelde activiteiten of activiteiten zijn hersteld, wordt de uitvaltijd gemeten vanaf het begin van het Incident tot het moment waarop die vertraagde dienst volledig wordt verleend. Het tijdstip dat de dienst uitviel is niet te bepalen, wordt de uitvaltijd gemeten vanaf het moment dat deze werd ontdekt.	Uitvaltijd van ICT-diensten die kritieke of belangrijke functies ondersteunen => 2 uur	
Geografische spreiding	Incident heeft gevolgen op: - Cliënten en financiële tegenpartijen in andere lidstaten; - Bijkantoren of andere financiële entiteiten binnen de groep die activiteiten verrichten in andere lidstaten; - Financiële marktinfrastucturen of derde aanbieders, die gevolgen kunnen hebben in andere lidstaten waaraan zij diensten verlenen, voor zover dergelijke informatie beschikbaar is.	De materialiteitsdrempel wordt bereikt wanneer het Incident gevolgen heeft op 2 of meer lidstaten.	
Gegevensverliezen	Beschikbaarheid van de gegevens: Gegevens zijn tijdelijk of permanent ontoegankelijk of onbruikbaar. Authenticiteit van gegevens: De betrouwbaarheid van de gegevensbron is in het gedrang gebracht. Integriteit van de gegevens: Incident heeft geleid tot niet-toegestane wijzigingen van gegevens waardoor die onjuist of onvolledig zijn geworden. Vertrouwelijkheid van gegevens: Gegevens zijn geraadpleegd door of vrijgegeven aan een niet-gemachtigde partij of systeem.	De materialiteitsdrempel wordt bereikt als aan een van de volgende criteria is voldaan: - Een effect op de criteria heeft een negatief effect of zal een negatief effect hebben op de verwezenlijking van de bedrijfsdoelstellingen of op het vermogen om aan de	

		regelgevingsvereisten te voldoen; Er is sprake van een succesvolle, kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen waarbij die toegang tot gegevensverliezen kan leiden.	- o het vastgestelde criterium inzake de mate waarin diensten als cruciaal kunnen worden aangemerkt; - o de materialiteitsdrempel voor cliënten, financiële tegenpartijen en transacties; - o de materialiteitsdrempel voor geografische spreiding.
Mate waarin getroffen diensten als cruciaal kunnen worden aangemerkt	Het Incident heeft gevolgen of heeft gehad voor ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen; Het Incident heeft gevolgen of heeft gehad voor financiële diensten waarvoor een vergunning of registratie vereist is of die onder toezicht staan van bevoegde autoriteiten; Het Incident heeft of vormt een succesvolle, kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen.		
Economische effecten	Voor het bepalen van de economische effecten houdt men rekening met de volgende directe en indirecte kosten en verliezen, zonder rekening te houden met financiële terugvorderingen: - onteigende gelden of financiële activa waarvoor zij aansprakelijk zijn, met inbegrip van door diefstal verloren gegane activa; - kosten voor de vervanging of verplaatsing van software, hardware of infrastructuur; - personeelskosten, met inbegrip van kosten in verband met de vervanging of verhuizing van personeel, de aanwerving van extra personeel, de bezoldiging voor overuren en het terugverdienen van verloren of verminderde vaardigheden; - vergoedingen wegens niet-naleving van contractuele verplichtingen; - kosten voor verhaal en compensatie voor klanten; - verliezen als gevolg van gederfde inkomsten; - kosten voor interne en externe communicatie; - advieskosten, met inbegrip van kosten in verband met juridisch advies, forensische diensten en saneringsdiensten.	Kosten en verliezen > 100 000 euro.	Wanneer het Fonds, afhankelijk van het soort Cyberdreiging en de beschikbare informatie, concludeert dat de materialiteitsdrempels voor Reputatieschade, Duur en uitvaltijd, Gegevensverliezen en Economische effecten kunnen worden bereikt, kunnen die drempels ook in aanmerking worden genomen.

	Kosten en verliezen voor de dagelijkse bedrijfsvoering worden niet in rekening gebracht. Deze zijn: - kosten voor algemeen onderhoud van infrastructuur, uitrusting, hardware en software, en kosten voor het up-to-date houden van de vaardigheden van het personeel; - interne of externe kosten om het bedrijf na het Incident te verbeteren, met inbegrip van upgrades, verbeteringen en risicobeoordelingsinitiatieven; - verzekeringspremies.		
--	--	--	--

Bijlage 4 Klokkenluidersregeling Stichting Pensioenfonds Thales Nederland

{OPEN}

Klokkenluidersregeling Stichting Pensioenfonds Thales Nederland

Inleiding

Deze klokkenluidersregeling bevat een procedure voor het melden van (een vermoeden van) misstanden binnen Stichting Pensioenfonds Thales Nederland (hierna: het Fonds).

De regeling bevat waarborgen voor de bescherming van alle personen die bij of voor het Fonds werken dan wel hebben gewerkt. Het Fonds vindt het heel belangrijk dat betrokkenen zich veilig voelen om hun zorgen te uiten. Deze klokkenluidersregeling legt uit hoe op een veilige manier vermoedens van misstanden intern en extern kunnen worden gemeld.

Met deze regeling geeft het Fonds uitvoering aan de vereisten van de Wet bescherming Klokkenluiders en de pensioenwetgeving.

Inhoudsopgave

1. Definities	3
2. Procedure melden misstand	5
3. Afhandelen misstanden	6
4. Rechtsbescherming.....	7
5. Publicatie en rapportage.....	7
6. Samenhang interne regelingen	8
7. Inwerkingtreding.....	8

1. Definities

Deze regeling volgt de definities uit de Wet bescherming Klokkenluiders (de Wet). Voor een goed begrip van deze regeling zijn enkele definities uit de Wet hieronder opgenomen, alsmede een toelichting op de definitie van benadeling:

Melder:

een natuurlijke persoon die in de context van zijn toekomstige, huidige of vroegere werk voor het Fonds een vermoeden van een misstand meldt of openbaar maakt.

Misstand:

- a) een schending of een gevaar voor schending van het Unierecht¹, of
- b) een handeling of nalatigheid waarbij het maatschappelijk belang in het geding is bij:
 - een schending of een gevaar voor schending van een wettelijk voorschrift of van interne regels die een concrete verplichting inhouden en die op grond van een wettelijk voorschrift door een werkgever zijn vastgesteld, dan wel
 - een gevaar voor de volksgezondheid, voor de veiligheid van personen, voor de aantasting van het milieu of voor het goed functioneren van de openbare dienst of een onderneming als gevolg van een onbehoorlijke wijze van handelen of nalaten².

Het maatschappelijk belang is in ieder geval in het geding indien de handeling of nalatigheid niet enkel persoonlijke belangen raakt en er sprake is van oftewel een patroon of structureel karakter dan wel de handeling of nalatigheid ernstig of omvangrijk is.

Betrokken derde:

- a) een derde die verbonden is met een melder en die kan worden benadeeld door de werkgever van de melder, of
- b) een persoon of organisatie waarmee de melder anderszins in een werkgerelateerde context verbonden is,
- c) een rechtspersoon die eigendom is van de melder, waarvoor de melder werkt of waarmee de melder anderszins werkgerelateerd verbonden is.

Benadeling:

omvat in ieder geval elke vorm van, dreiging of poging tot ontslag of schorsing, een boete als bedoeld in artikel 650 van Boek 7 van het Burgerlijk Wetboek, demotie, het onthouden van bevordering, een negatieve beoordeling, een schriftelijke berisping, overplaatsing naar een andere vestiging, discriminatie, intimidatie, pesterijen of uitsluiting, smaad of laster, voortijdige beëindiging van een overeenkomst voor het leveren van goederen of diensten.

Compliance Officer:

De functionaris die als Compliance Officer is benoemd of indien er geen Compliance Officer benoemd is, degene die verantwoordelijk is voor het uitvoeren van de compliancewerkzaamheden.

Mevrouw S. Holwerda, arbeidsjuriste.

¹ Onder Unierecht valt Europese regelgeving op het gebied van onder meer overheidsopdrachten, financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering, productveiligheid en productconformiteit, veiligheid van het vervoer, bescherming van het milieu, stralingsbescherming en nucleaire veiligheid, veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn, volksgezondheid, consumentenbescherming, bescherming van de persoonlijke levenssfeer.

² Het gaat hier om een direct aan Stichting Pensioenfonds Thales Nederland toe te rekenen gedraging die tot de misstand leidt, dus niet bijvoorbeeld het Fonds in haar rol van institutioneel belegger of aandeelhouder

Verbonden personen:

- a. leden van het bestuur,
- b. leden van de Raad van Toezicht en het Verantwoordingsorgaan;
- c. externe leden van commissies die zijn ingesteld ter ondersteuning van het bestuur,
- d. medewerkers van het bestuursbureau, waaronder mensen die tijdelijk werken/inhuur,
- e. andere (groepen van) personen die door het bestuur worden aangewezen,
- f. sleutelfunctiehouders en de vervullers van de sleutelfuncties.

2. Procedure melden misstand

De melding wordt gedaan bij de Compliance Officer.

Het heeft de voorkeur dat de melder zijn melding intern doet. De melder is echter niet verplicht om een melding van een vermoeden van een misstand eerst intern te melden. De melder kan daarvan ook direct een externe melding doen bij een bevoegde autoriteit.

Verder kan de melder ook kiezen voor een externe melding als:

- De melder het niet eens is met het standpunt van het Fonds of van oordeel is dat de melding ten onrechte terzijde is gelegd of onvoldoende onderzocht is of;
- De melder niet binnen 3 maanden na de verzending van de ontvangstbevestiging van zijn melding een standpunt heeft ontvangen over de interne melding.

De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. De melder heeft de mogelijkheid om de melding te doen via een gesprek op locatie. Dat gesprek dient op redelijke termijn na ontvangst van het verzoek plaats te vinden.

Bij een mondelinge melding, al dan niet op locatie, registreert het Fonds de melding door een opname of een schriftelijk verslag van het gesprek te maken. De melder wordt in de gelegenheid gesteld het verslag te controleren, aan te vullen en voor akkoord te tekenen.

De ontvanger van de melding draagt er zorg voor dat de melder binnen zeven dagen een ontvangstbevestiging ontvangt en stelt het dagelijks bestuur, door middel van een afschrift van de vastlegging van de melding, op de hoogte van de melding. De naam van de melder wordt alleen bekendgemaakt met toestemming van de melder of wanneer daartoe een wettelijke verplichting bestaat. Ingeval enig wettelijk voorschrift tot mededeling van de identiteit van een melder verplicht, dan wordt de melder daarvan in kennis gesteld.

De Compliance Officer beoordeelt of de melding kwalificeert als het vermoeden van een misstand zoals bedoeld in deze regeling en in de Wet bescherming Klokkenluiders. Wanneer de melding kwalificeert als een misstand informeert de Compliance Officer het dagelijks bestuur over de melding en adviseert hen over het op te starten onderzoek. Bij twijfel overlegt de Compliance Officer met de sleutelfunctiehouder risicobeheer.

Indien de misstand tevens kwalificeert als een integriteitsincident in de zin van de Incidentenregeling dan zal het Fonds op grond van die regeling ook een melding aan de toezichthouder moeten doen. De uitgangspunten rondom vertrouwelijkheid gelden in dat geval onverkort.

Het dagelijks bestuur besluit over de vervolgstappen en de wijze van onderzoek. Ook worden de overige bestuursleden en de raad van toezicht op de hoogte gebracht van de melding. Het besluit tot verder onderzoek en de gronden waarop het gebaseerd is wordt binnen twee weken na de melding genomen en schriftelijk aan de melder meegedeeld.

Wanneer de melding niet kwalificeert als een misstand, beoordeelt de Compliance Officer wie de melding namens het Fonds verder afhandelt. De Compliance Officer informeert de melder binnen twee weken na de melding gemotiveerd over de beoordeling en over de verdere afhandeling.

Een melder kan een adviseur in vertrouwen raadplegen over een vermoeden van een misstand. Ook kan een melder een vertrouwenspersoon via Paradigma (telefonisch te bereiken via 088-032 2400), of de afdeling Advies van het Huis voor Klokkenluiders (telefonisch te bereiken via 088-1331 030) verzoeken om informatie, advies en ondersteuning in verband met het vermoeden van een misstand.

Wanneer de melder zijn melding geheel anoniem wil doen, dan kan de melder een tijdelijk e-mailadres aanmaken, waarmee met de Compliance Officer gecommuniceerd kan worden.

Een melder heeft de mogelijkheid om een melding van een misstand openbaar te maken.

Openbaarmaking is alleen toegestaan:

- a. als de melder redelijke gronden heeft om aan te nemen dat de gemelde informatie over het vermoeden van een misstand op het moment van openbaarmaking juist is; én
- b. als de melder voorafgaand aan de openbaarmaking melding heeft gedaan bij de Compliance Officer; of
- c. als de melder voorafgaand aan de openbaarmaking melding heeft gedaan bij het dagelijks bestuur/voorzitter van de raad van toezicht; én
- d. als de melder redelijke gronden heeft om aan te nemen dat het onderzoek naar het vermoeden van een misstand onvoldoende voortgang heeft.

Een melding op grond van deze regeling en de beoordeling van de melding worden geregistreerd in een register. Gedurende het verdere proces worden in het dossier de relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek. De gegevens worden vernietigd op het moment dat deze niet meer noodzakelijk zijn dan wel indien enig wettelijk voorschrift dit voorschrijft.

De Compliance Officer zorgt ervoor dat informatie over de melding alleen toegankelijk is voor diegenen die bij de melding betrokken zijn.

3. Afhandelen misstanden

Het dagelijks bestuur draagt het onderzoek op aan onderzoekers die onafhankelijk en onpartijdig zijn. Het onderzoek kan intern worden uitgevoerd of door een extern bureau.

De onderzoekers stellen de melder in de gelegenheid te worden gehoord. Hiervan wordt verslag gemaakt. Indien akkoord bevonden, tekent de melder het verslag voor goedkeuring en ontvangt een kopie. De onderzoekers kunnen ook anderen horen. Ook hiervan wordt verslag gemaakt. Diegene die gehoord is, tekent het verslag indien akkoord bevonden voor goedkeuring en ontvangt hiervan een kopie.

De onderzoekers kunnen binnen het Fonds alle documenten en gegevens opvragen en inzien die zij voor het onderzoek redelijkerwijs noodzakelijk vinden, met inachtnaam van het privacybeleid van het Fonds.

De melder mag de onderzoekers alle documenten en gegevens verstrekken waarvan hij het redelijkerwijs nodig vindt dat de onderzoekers daar kennis van nemen.

De onderzoekers stellen een concept onderzoeksrapport op. De melder krijgt de gelegenheid om daar opmerkingen bij te maken, tenzij hiertegen ernstige bezwaren bestaan. De onderzoekers stellen vervolgens het onderzoeksrapport vast en stellen dit rapport ter beschikking aan het dagelijks bestuur.

De hierboven genoemde werkzaamheden vinden plaats binnen drie maanden na ontvangst van de melding. De Compliance Officer houdt de melder op de hoogte van de voortgang in het dossier, bijvoorbeeld door het sturen van een periodiek voortgangsbericht.

Het dagelijks bestuur deelt het onderzoeksrapport zo spoedig mogelijk met de rest van het bestuur. Het bestuur besluit binnen een redelijke termijn na ontvangst van het onderzoeksrapport of en zo ja welke maatregelen genomen worden en welke personen/fondsgremia en/of externe instanties geïnformeerd worden over het onderzoeksrapport en/of de genomen maatregelen.

Indien de melder het niet eens is met de uitkomst in het onderzoeksrapport of de manier waarop de melding wordt opgepakt en onderzocht, dan kan de melder zich met zijn zorg wenden tot de raad van toezicht. De raad van toezicht neemt passende maatregelen en informeert de melder hierover.

4. Rechtsbescherming

Het Fonds draagt er zorg voor dat de melder op geen enkele wijze in zijn (arbeidsrechtelijke) positie bij het Fonds benadeeld wordt, voor zover deze te goeder trouw gehandeld heeft. Het Fonds gaat er van uit dat een melding te goeder trouw is gedaan, tot het moment dat hij overtuigd is geraakt van het tegendeel.

Als de melder van mening is dat sprake is van benadeling kan de melder:

- De Compliance Officer verzoeken om onderzoek te (laten) doen naar de wijze waarop er met de melder is omgegaan; en/of;
- Hierover advies inwinnen bij de afdeling advies van het Huis voor Klokkenluiders; en/of;
- Een bejegeningsonderzoek aanvragen bij de afdeling onderzoek van het Huis voor Klokkenluiders.

Represailles als gevolg van melden worden beschouwd als een ernstige schending van deze klokkenluidersregeling, in welk geval door het bestuur passende actie zal worden ondernomen om de (arbeidsrechtelijke) positie van de melder te beschermen.

Het Fonds draagt er zorg voor dat de Compliance Officer op geen enkele wijze in zijn positie bij het Fonds benadeeld wordt vanwege het uitoefenen van zijn taken op grond van deze regeling.

Een melder die willens en wetens heeft deelgenomen aan of veroorzaker is van een misstand, zal bij melding van deze misstand geen recht kunnen ontlenen aan de beschermingsregels zoals die gelden voor een te goeder trouw handelende melder.

In geval van intrekking van de misstand door de melder vergewist het Fonds zich ervan dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

De bepalingen in dit artikel gelden ook voor degene die de melder bijstaat en voor betrokken derden.

5. Publicatie en rapportage

Het Fonds zorgt ervoor dat deze regeling intern wordt gepubliceerd en op de website wordt geplaatst.

De Compliance Officer stelt jaarlijks een rapportage op over de uitvoering van deze regeling. De rapportage omvat in ieder geval informatie over het aantal en soort meldingen, de uitkomsten van de onderzoeken en de standpunten van het Fonds. Het bestuur bespreekt deze rapportage.

6. Samenhang interne regelingen

Er bestaan binnen het Fonds verschillende regelingen, processen en procedures (bijvoorbeeld de Gedragscode, de Incidentenregeling en de Regeling ongewenst gedrag op het werk). Ook in deze regelingen zijn gedragsnormen opgenomen. Deze conflicteren niet met de Klokkenluidersregeling en zijn eveneens van toepassing.

De samenhang tussen de verschillende regelingen is als volgt:

- Iedere Verbonden Persoon die een (dreigend) Incident constateert is gehouden dit te melden aan de Compliance Officer.
- Indien het belang van de onderneming, van derden of de bescherming van de eigen positie van de Verbonden persoon dit vraagt (bijvoorbeeld omdat hij vreest dat een melding nadelige gevolgen kan hebben voor zijn positie of indien aan een eerdere melding geen gevolg is gegeven), wordt het incident door de Verbonden persoon gemeld bij de Compliance Officer als Misstand conform de Klokkenluidersregeling. Het oordeel van de Verbonden persoon dat een melding dient plaats te vinden conform de Klokkenluidersregeling is daarbij doorslaggevend.
- Ongewenste gedragingen van een andere Verbonden persoon kunnen worden gemeld als Klacht bij de Vertrouwenspersoon conform de Regeling ongewenst gedrag op het werk.

7. Inwerkingtreding

Deze klokkenluidersregeling treedt in werking op 16-05-2025 en vervangt de vorige versie van 23-09-2015.

VERSIE BEHEER

Historie

Versie	Datum	Wijzigingen/Bijzonderheden	Auteur
Klokkenluidersregeling Stichting Pensioenfonds Thales Nederland.docx	23-09-2015	Laatste vastgestelde versie	Dolinda Buijnsters
Gewijzigd in 2025_Klokkenluidersregeling.docx			

Review

Versie	Datum	Wijzigingen/Bijzonderheden	Opsteller/Reviewer
2025_Klokkenluidersregeling.docx	16-05-2025	Aangepast conform nieuwe richtlijnen van pensioenfederatie	Leyla Katalanc

Vaststelling

Versie	Datum	Functie/Gremium	Vaststeller/Gremium
2025_Klokkenluidersregeling.docx	16-05-2025	Bestuur	Bestuur

Bijlage 5 Regeling vergoedingen organen van Stichting Pensioenfonds Thales Nederland (SPTN)

De organen van het pensioenfonds bestaan uit Bestuur, het VerantwoordingsOrgaan en de Raad van Toezicht.

De taak van de bestuurders van SPTN is het besturen van het pensioenfonds in al zijn facetten. Het bestuur bepaalt het beleid rondom de uitvoering, de financiering en de communicatie van de pensioenregeling. Daarnaast zijn er verschillende bestuurscommissies. Er is een communicatie commissie, een beleggingsadviescommissie en een risk commissie naast een dagelijks bestuur. De commissies en het dagelijks bestuur richten zich op specifieke aandachtsgebieden. Tevens worden externe vergaderingen, seminars en bijeenkomsten bijgewoond als vertegenwoordiger van het pensioenfonds. Ook volgen de bestuursleden elk jaar trainingen en opleidingen om bij te blijven in hun vakgebied.

Aan het VerantwoordingsOrgaan legt het Bestuur verantwoording af over beleid en de wijze waarop het is uitgevoerd. De Raad van Toezicht houdt toezicht op het beleid van het bestuur en op de algemene gang van zaken in het fonds.

De Regeling Vergoedingen voldoet aan de Pensioenwet en SPTN past de Code Pensioenfondsen (wettelijk verankerd in Wet Versterking Bestuur Pensioenfondsen) toe. Deze regels schrijven voor dat pensioenfondsen een beheerst en duurzaam beloningsbeleid voeren. Het fonds legt het beleid met betrekking tot beloning schriftelijk vast en maakt dit ook openbaar door middel van plaatsing op de website. De Regeling Vergoedingen voldoet tevens aan artikel 21a van het Besluit Financieel Toetsingskader die pensioenfondsen verplicht tot het voeren van een beheerst beloningsbeleid. Het fonds past de DNB/AFM Principes voor Beheerst Beloningsbeleid toe. De volgende vergoedingsregeling voor de organen van het fonds is vastgesteld:

Artikel 1: Vergoedingen Bestuur

Het bestuurslidmaatschap betreft een onbezoldigde functie. Kosten van opleiding en deskundigheidsbevordering ten behoeve van het bestuurslidmaatschap en reis- en verblijfkosten in verband met opleiding of het bezoek van seminars en congressen worden vergoed volgens de specificatie in bijlage I.

{OPEN}

Artikel 2: Vergoedingen VerantwoordingsOrgaan

Het lidmaatschap van het VerantwoordingsOrgaan betreft een onbezoldigde functie. Kosten van opleiding ten behoeve van het lidmaatschap en reis- en verblijfkosten in verband met opleiding of het bezoek van seminars en congressen worden vergoed volgens de specificatie in bijlage I.

Artikel 3: Vergoedingen Raad van Toezicht

- a. Leden van de Raad van Toezicht ontvangen een vergoeding voor hun werkzaamheden. De vergoeding is nader gespecificeerd in bijlage I.
- b. Ter compensatie van extra werkzaamheden ontvangt de voorzitter een hogere vergoeding.

Artikel 4: Slotopmerkingen

- a. Dit beleid inzake vergoedingen voor organen van SPTN wordt vastgesteld door het Bestuur en ter advies voorgelegd aan het Verantwoordingsorgaan.
- b. Dit beleid inzake vergoedingen voor organen van SPTN wordt ter goedkeuring voorgelegd aan de Raad van Toezicht, behoudens de vergoedingen voor de Raad van Toezicht.
- c. Alleen kosten genoemd in deze regeling komen voor vergoeding in aanmerking.
- d. Wanneer onverkorte toepassing van deze regeling tot onredelijkheid leidt, kan het Bestuur een beslissing nemen die afwijkt van de bepalingen in deze regeling.
- e. In onvoorziene gevallen beslist het Bestuur.

Artikel 5: Inwerkingtreding

Deze regeling is per 18 juni 2021 met terugwerkende kracht in werking getreden, en vastgesteld per 24 september 2021 (door Bestuur na advies VO). De regeling geldt voor een periode van 3 jaar.

Artikel 6: Citeertitel

Deze regeling wordt aangehaald als Regeling Vergoedingen.

Bijlage I Specificatie van de vergoedingen

Artikel 1: Vergoedingen Bestuur

Kosten van opleiding en deskundigheidsbevordering worden volledig vergoed door SPTN. Het Bestuur stemt hierover af en stelt hier jaarlijks een budget voor vast.

Reis- en verblijfkosten in verband met opleiding of het bezoek van seminars, congressen en andere voor de bestuurswerkzaamheden noodzakelijke externe vergaderingen worden vergoed op basis van werkelijk gemaakte reiskosten per kilometer cq. werkelijk gemaakte verblijfkosten (specificeren met bonnen/facturen). Voor bestuurders met een dienstverband bij Thales gelden de reis- en verblijfkosten regelingen van Thales. De kosten komen ten laste van de werkgever.

Voor bestuurders zonder dienstverband bij Thales geldt per 1 januari 2023 een onbelaste vaste onkostenvergoeding van € 1.000 per jaar. Deze onkostenvergoeding zal jaarlijks in de maand juli worden uitbetaald. Daarnaast worden de gemaakte reiskosten vergoed op basis van de maximaal fiscaal onbelaste kilometervergoeding. De onbelaste onkostenvergoeding zal jaarlijks worden geïndexeerd met hetzelfde percentage waarmee de belastingdienst de fiscaal maximale onbelaste onkostenvergoeding ophoogt (2023: €1.900,- per jaar).

Artikel 2: Vergoedingen VerantwoordingsOrgaan

Kosten van opleiding en deskundigheidsbevordering worden volledig vergoed door SPTN. Het verantwoordingsorgaan stemt hierover af en stelt een budget voor aan het bestuur. Het Bestuur stelt het opleidingsbudget jaarlijks vast.

Reis- en verblijfkosten in verband met opleiding of het bezoek van seminars en congressen worden vergoed op basis van werkelijk gemaakte reiskosten per kilometer cq. werkelijk gemaakte verblijfkosten (specificeren met bonnen/facturen). Voor leden van het VerantwoordingsOrgaan met een dienstverband bij Thales gelden de reis- en verblijfkosten regelingen van Thales. De kosten komen ten laste van de werkgever.

Voor leden van het VerantwoordingsOrgaan zonder dienstverband bij Thales geldt per 1 januari 2023 een onbelaste vaste onkostenvergoeding van € 1.000 per jaar. Deze onkostenvergoeding zal jaarlijks in de maand juli worden uitbetaald. Daarnaast worden de gemaakte reiskosten vergoed op basis van de maximaal fiscaal onbelaste kilometervergoeding.

De onbelaste onkostenvergoeding zal jaarlijks worden geïndexeerd met hetzelfde percentage waarmee de belastingdienst de fiscaal maximale onbelaste onkostenvergoeding ophoogt (2023: €1.900,- per jaar).

Artikel 3: Vergoedingen Raad van Toezicht

De vergoeding van de Raad van Toezicht is als volgt vastgesteld: € 13.200 vaste vergoeding per jaar voor een lid en € 15.400 vaste vergoeding per jaar voor de voorzitter. Daarnaast geldt een vaste vergoeding als tegemoetkoming in reis- en verblijfkosten van € 550 per jaar voor leden en de voorzitter. Alle bedragen en facturen zijn exclusief BTW.

De vergoeding van RVT leden zal geïndexeerd worden. Per 1 december 2022 zal dit van kracht worden. De vergoeding van RvT leden zal opgehoogd worden met de structurele ontwikkeling van het salaris volgens de CAO Metalektro (zonder eenmalige uitkeringen) die ingaan op het moment van de verhoging voor het CAO personeel. Ter informatie: per 1 december 2022 stijgen de lonen met 5,5% en per 1 januari 2024 met 3,5%.

Eventuele vergoedingen aan derden door de voorzitter of een lid (bijvoorbeeld aan VCP) zijn in deze bedragen inbegrepen.

In het geval van buitengewone werkzaamheden (vooraf overeen te komen tussen Raad van Toezicht en het Bestuur) zal een separaat contract worden opgesteld.

VERSIE BEHEER

Historie

Versie	Datum	Wijzigingen/Bijzonderheden	Auteur
Regeling vergoedingen organen SPTN_2021_def	01-12-2021	Bron document	Pensioenbureau
230616_Regeling vergoedingen organen SPTN_def	16-06-2023	Bestuur gaat over tot vaststelling van beleidsstuk na ontvangst van advies VO op 24 mei 2023.	Bestuur

Review

Versie	Datum	Functie/ Gremium	Reviewer
230630_Regeling vergoedingen organen SPTN_concept aanp onkostenvergoeding gepensioneerden_	30-06-2023	Ter review voorgelegd aan het DB	DB
230922_Regeling vergoedingen organen SPTN_aanp onkostenvergoeding gepensioneerden_concept	22-09-2023	Voorgenomen besluit	Bestuur

Vaststelling

Versie	Datum	Functie/Gremium	Vaststeller/Gremium
231117_Regeling vergoedingen organen SPTN_def	17-11-2023	Bestuur aanpassing vastgesteld	Bestuur

Bijlage 6 Compliance rapportage

In deze periodieke compliance rapportage over de periode rapporteert de Compliance Officer aan het Bestuur van Stichting Pensioenfonds Thales Nederland over de stand van zaken met betrekking tot compliance.

De rapportage heeft de volgende twee doelen:

- inzicht bieden in de compliance-incidenten;
- beheersing van de belangrijkste compliance thema's en -risico's.

Incidentele rapportages

In het geval van ernstige compliance-incidenten wordt direct gerapporteerd, zowel in de hiërarchische als in de functionele compliancelijn. Bij deze rapportage kan gedacht worden aan de volgende issues:

- elke schending van wet- en regelgeving of ethische standaard die op zichzelf of in combinatie met andere overtredingen een negatief effect op de reputatie van de Stichting Pensioenfonds Thales Nederland kan hebben;
- het bewust achterhouden van informatie over ongewenste handelingen of situaties;
- laakbaar gedrag in integriteitkwesties;
- elk voorval waarvan de Compliance Officer oordeelt dat het belang van de zaak directe rapportage rechtvaardigt.

Kleinere incidenten worden gerapporteerd in de compliance rapportage aan de voorzitter van het pensioenfonds.

Rapportage Compliance Officer periode xxxx - xxxx:

In deze periodieke compliance rapportage rapporteert de Compliance Officer over een bepaalde periode aan het bestuur van Stichting Pensioenfonds Thales Nederland over de stand van zaken met betrekking tot compliance. De input voor deze rapportage vormt de basis van de activiteiten van het pensioenfonds.

<u>1.Compliance-monitoring activiteiten:</u>	Datum	Toelichting/ Opmerkingen
Aanwezigheid actueel geschiktheidsplan met een overzicht van de gevolgde opleidingen/cursussen en gemaakte toetsen.		
Aanwezigheid ondertekende gedragscodes van alle verbonden personen.		
Jaarlijkse bevestiging van externe partijen (voor pensioenadministratie en vermogensbeheer) voor het compliant zijn: AON Hewitt BV		
NN IM		
BlackRock		
Kasbank		
Financiële gegevens van het Pensioenfonds gecontroleerd door de accountant		
Actuariële gegevens en grondslagen gecontroleerd door de certificerend actuaris		
Heeft het bestuur de jaarlijkse ISAE 3402 rapporten van de gecontracteerde service providers beoordeeld		
Zijn de SLA-rapporten van de pensioenuitvoerder door het bestuur beoordeeld.		
Is er een rapport van de visitatiecommissie		
Is er een oordeel van het verantwoordingsorgaan		
Is er een informatiebijeenkomst georganiseerd		
Periodiek bespreken notitie Risicomanagement in bestuursvergadering.		

<u>2. Compliance-bewustzijns activiteiten:</u>	Datum	Opmerkingen

Periodieke agendering van compliance/ integriteit in de bestuursvergadering		
Jaarlijkse bespreking met compliance officer, manager pensioenbureau en (een delegatie van) het bestuur		
Jaarlijkse evaluatie bestuur Pensioenfonds		

<u>3. Compliance-incidenten</u>				
Lopend aantal	Aantal nieuw gemeld	Aantal Afgehandeld	Lopend aantal ultimo huidige periode	Aantal gemeld toezichthouder
Toelichting				

Nieuwe wet- en regelgeving. Onderstaand de belangrijkste actualiteiten op het gebied van wet – en regelgeving.	Status

{OPEN}