

Stichting Bedrijfstakpensioenfond voor Vlees, Vleeswaren, Gemaksvoeding en Pluimveevlees

Gedragscode

ingevolge

**artikel 5:68 Wet op het financieel toezicht en
artikel 20 Besluit financieel toetsingskader pensioenfondsen**

Artikel 1 Definities

- 1.1 Verbonden personen zijn:
- leden van het bestuur,
 - leden van de raad van toezicht,
 - leden van het verantwoordingsorgaan,
 - andere personen die door het bestuur zijn aangewezen, waaronder in ieder geval medewerkers van Actor Partner in Besturen voor zover zij werkzaamheden verrichten voor Stichting Bedrijfstakpensioenfond voor Vlees, Vleeswaren, Gemaksvoeding en Pluimveevlees. (hierna: VLEP).
- 1.2 Insiders zijn:
verbonden personen, die direct of indirect bij transacties van VLEP 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.
- VLEP kent geen insiders, zodra hiervan sprake is wordt de gedragscode hierop aangepast.
- 1.3 Gelieerde derden zijn:
- echtgenoot, echtgenote of partner van de verbonden persoon,
 - bloed- en aanverwanten tot de tweede graad van de verbonden persoon,
 - (andere) personen die tot het huishouden van de verbonden persoon behoren,
- 1.4 Nevenfunctie:
Activiteit of werkzaamheden die een verbonden persoon (betaald of onbetaald) naast zijn hoofdberoep of bezigheid uitvoert. In het kader van deze gedragscode geldt de functie die de verbonden persoon voor VLEP uitvoert als hoofdfunctie, ongeacht de verhouding in beslag met eventuele andere bezigheden.
- 1.5 Integriteitsrisico is:
gevaar voor de aantasting van de goede reputatie, alsmede de bestaande en toekomstige bedreiging van het vermogen of resultaat van VLEP, als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift, interne procedure en/of gedragsregel is voorgeschreven.
- 1.7 Reputatierisico is:
gevaar voor de aantasting van de goede reputatie van VLEP.
- 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 VLEP 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 Waar in deze gedragscode staat geschreven 'hij' of 'zijn' moet tevens worden gelezen 'zij' of 'haar'.
- 1.11 Indien volgens deze gedragscode de voorzitter van het bestuur toestemming of goedkeuring nodig heeft, dan wordt toestemming gevraagd aan de sleutelfunctiehouder risicomanagement.

Artikel 2 Inleidende bepalingen

- 2.1 Het doel van de gedragscode is het waarborgen en handhaven van het vertrouwen in VLEP door belanghebbenden, door gewenst gedrag te stimuleren en ongewenst gedrag te voorkomen. De gedragscode kent daartoe algemene gedragsregels voor verbonden personen.
- 2.2 De gedragscode bevordert de transparantie rondom gedragsregels en maakt duidelijk aan alle bij VLEP verbonden personen – ook voor de bescherming van hun eigen belangen – wat wel en wat niet is geoorloofd.
- 2.3 De gedragscode draagt mede bij aan het integer functioneren van VLEP ten behoeve van al diegenen die bij VLEP belang hebben en het waarborgen van de goede naam en reputatie van VLEP en de pensioensector in het algemeen.
- 2.4 VLEP handelt op een ethische en sociaal verantwoorde manier en houdt zich aan de mensen- en kinderrechten, de toepasselijke principes inzake milieubescherming, en zorgt voor passende arbeidsomstandigheden.
- 2.5 Het is niet toegestaan de normen van de gedragscode te omzeilen door het betrekken van (gelieerde) derden.
- 2.6 Verbonden personen van VLEP en uitbestedingspartijen zijn verplicht zich op de hoogte te stellen van, en zich te houden aan de beleidsstukken inzake informatiebeveiliging, waaronder het AI-beleid en de gedragsrichtlijn Veilig en Bewust Digitaal Werken. VLEP stelt daartoe de benodigde informatie beschikbaar aan de verbonden personen en uitbestedingspartijen
- 2.7 De organisatie waaraan VLEP werkzaamheden heeft uitbesteed moet beschikken over een gedragscode, die ten minste gelijkwaardig is aan die van VLEP.
- 2.8 Het bestuur van VLEP is verantwoordelijk voor het naleven van de verplichtingen die voortvloeien uit enige wettelijke bepaling of de gedragscode.

Artikel 3 Normen over 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 te melden bij

de voorzitter. De voorzitter kan toestemming verlenen en maakt zijn antwoord tevens kenbaar aan de vicevoorzitter en de compliance officer.

De verbonden persoon is niet verplicht melding te doen als hij handelt vanuit een reeds gemelde en goedgekeurde nevenfunctie en het geval deel uit maakt van het bekleden van de functie, tenzij het een (potentieel) belangenconflict betreft. De verbonden persoon dient hierbij te allen tijde bij aanvaarding te vermelden in welke hoedanigheid hij handelt.

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. financiële belangen in zakelijke belangen;
5. pensioenfondseigendommen; en
6. leveranciers en dienstverleners.

3.1 Relatiegeschenken

De verbonden persoon dient terughoudend en transparant om te gaan met het aanvaarden van relatiegeschenken om te voorkomen dat (de schijn ontstaat dat) het aanvaarden van een relatiegeschenk van invloed kan zijn op beslissingen van VLEP. 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 , en
- onmiddellijke melding van mogelijke beïnvloeding met behulp van een relatiegeschenk door (toekomstige) relaties van VLEP .

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

3.2 Uitnodigingen

Uitgangspunten voor uitnodigingen zijn:

- alleen uitnodigingen waarop de verbonden persoon in wenst te gaan dienen te worden gemeld;
- (aspirant) leden van het bestuur melden de uitnodiging mondeling tijdens een bestuursvergadering voorafgaand aan het event, waarbij gelijktijdig de uitnodiging door het bestuur kan worden goedgekeurd;
- de overige verbonden personen melden bij de bestuursvoorzitter(s) en/of compliance officer, zij dragen er zorg voor dat de vereiste goedkeuring kan worden verleend;
- de compliance officer kan gevraagd en ongevraagd advies geven op het al dan niet accepteren en/of goedkeuren van de uitnodiging;
- er wordt terughoudend omgegaan met repeterende uitnodigingen;
- uitnodigingen voor webinars zijn uitgezonderd van de meldplicht.

3.2.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 VLEP wordt aangetoond; en
- de uitnodiging vooraf is goedgekeurd door het bestuur.

3.2.b. Congressen en seminars

Uitnodigingen voor congressen en seminars mogen worden aanvaard indien:

- er geen sprake is van een potentieel belangenconflict,
- goedkeuring is verleend door het bestuur.

Uitnodigingen voor seminars, congressen, trainingen e.d., bedoeld om kennis te vergaren over ontwikkelingen en actuele onderwerpen voor VLEP en/of de pensioensector zijn uitgezonderd van de meldplicht, behalve wanneer de uitnodiging overdreven is aangekleed (denk aan soort locatie, eten, aanwezig entertainment, e.d) Bij twijfel kan de compliance officer geraadpleegd worden.

3.2.c. Evenementen

Uitnodigingen voor entertainment (bijvoorbeeld sportwedstrijden en concerten) mogen worden aanvaard indien:

- er geen sprake is van een potentieel belangenconflict;
- het zakelijke karakter en het belang voor VLEP wordt aangetoond; en
- de uitnodiging vooraf is goedgekeurd door het bestuur.

3.2.d. Spreker congres

Uitnodigingen om als spreker namens VLEP 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;
- er vooraf goedkeuring is gegeven door het bestuur/voorzitter.

3.3 Nevenfuncties

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

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 VLEP,
- kan leiden tot reputatieschade voor VLEP.

De voorzitter doet tevens melding van de nevenfunctie bij de compliance officer.

3.4 Financiële belangen in zakelijke relaties

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

3.5 Pensioenfondseigendommen

De verbonden persoon gaat zorgvuldig om met de bedrijfsmiddelen van VLEP. Het gebruik van bedrijfsmiddelen vindt plaats overeenkomstig de Regeling gebruik pensioenfondseigendommen en de Gedragsrichtlijn Veilig en Bewust Digitaal Werken.

3.6 Leveranciers en dienstverleners

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

Artikel 4 Normen over voorwetenschap

- 4.1 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 De verbonden persoon, anders dan de insider, die beschikt over informatie als bedoeld in artikel 4.1, 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.
- 4.3 Iedere verbonden persoon is desgevraagd gehouden alle informatie aan de compliance officer te verschaffen in het kader van de strikte naleving van de gedragscode.

Artikel 5. Vertrouwelijkheid

- 5.1 De verbonden persoon mag geen informatie over zaken – inclusief individuele pensioengegevens en beleggingen – van VLEP of contractspartijen van VLEP, 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 VLEP gebruiken.

Het gebruik van AI-toepassingen vindt plaats overeenkomstig het AI-beleid van VLEP. Vertrouwelijke informatie, persoonsgegevens en andere niet-openbare informatie mogen uitsluitend in AI-toepassingen worden verwerkt indien dit is toegestaan op grond van het AI-beleid en overige toepasselijke beleidsdocumenten van het VLEP.

Indien de verbonden persoon gebruik maakt van een eigen tablet, laptop, desktop, smartphone of ander elektronisch apparaat voor het inzien en verwerken van informatie van VLEP, dient het apparaat te voldoen aan de eisen zoals opgenomen in de Gedragsrichtlijn Veilig en Bewust Digitaal Werken (Bijlage 2). De verbonden persoon is verantwoordelijk voor de naleving hiervan.

Artikel 6 Meldingsplicht

- 6.1 Iedere verbonden persoon is verplicht elk (potentieel) tegenstrijdig belang of reputatierisico te melden aan de voorzitter, die dit meldt aan de vice-voorzitter en de compliance officer. Pogingen van een (aspirant-)relatie tot beïnvloeding dienen eveneens onverwijld te worden gemeld.
- 6.2 Beveiligingsincidenten, phishingpogingen, verlies van apparatuur, ongeautoriseerde toegang tot gegevens en andere digitale incidenten worden gemeld overeenkomstig de incidentenregeling van VLEP en de Gedragsrichtlijn Veilig en Bewust Digitaal Werken.

Artikel 7 Compliance officer

- 7.1 VLEP wijst een compliance officer aan. De compliance officer vervult een onafhankelijke rol binnen VLEP. De compliance officer wordt benoemd door het bestuur van VLEP. De compliance officer rapporteert aan de voorzitter van de bestuur, zowel voor de dagelijkse gang van zaken, als in het geval zich een bijzondere omstandigheid heeft voorgedaan.

- 7.2 Het bestuur van VLEP 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. De externe accountant ziet toe op de in het kader van de naleving van de gedragscode door de compliance officer uitgevoerde werkzaamheden.
- 7.3 Het bestuur legt vast welke acties zijn ondernomen naar aanleiding van de bevindingen van de compliance officer.
- 7.4 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.
- 7.5 De compliance officer adviseert en informeert, gevraagd én ongevraagd, verbonden personen over de uitleg en toepassing van de gedragscode.
- 7.6 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.
- 7.7 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.
- 7.8 De compliance officer en de voorzitter van het bestuur zijn gehouden tot geheimhouding van de informatie verstrekt door verbonden personen of derden. De geheimhouding kan worden doorbroken in het geval de goede uitoefening van zijn functie daartoe noodzaakt.

Artikel 8 Ondertekening gedragscode en jaarlijkse verklaring

- 8.1 Iedere verbonden persoon moet bij aanvang van zijn functie bij VLEP de gedragscode ondertekenen, waarmee hij zich verbindt alle voor hem relevante regels uit deze gedragscode na te leven. Onder deze gedragscode vallen tevens de Regeling gebruik pensioenfondseigendommen (Bijlage 1) en de Gedragsrichtlijn Veilig en Bewust Digitaal Werken (Bijlage 2). Verbonden personen verklaren deze documenten te kennen en na te leven.
- 8.2 Aan het eind van ieder kalenderjaar of bij het niet langer verbonden zijn aan VLEP, moet iedere verbonden persoon een verklaring ondertekenen over de juiste naleving van de geldende bepalingen in de gedragscode over het afgelopen jaar, inclusief de voorwaarden zoals vastgelegd in de 'Regeling gebruik pensioenfondseigendommen'. Bij het niet langer verbonden zijn aan VLEP blijven de uit de gedragscode geldende normen van toepassing op de verbonden persoon, voor zover dat uit hun aard voortvloeit.

Artikel 9 Sancties

- 9.1** Het handelen door de verbonden persoon in strijd met de gedragscode of het beleid inzake Informatiebeveiliging zoals aangegeven in het IT-beleid, AI-Beleid en de gedragslijn 'veilig en bewust Digitaal Werken' wordt beschouwd als een ernstige inbreuk op het vertrouwen dat VLEP in de betrokkene moet kunnen stellen. Een dergelijk handelen kan reden zijn tot het opleggen van een sanctie, afhankelijk van de ernst van de overtreding, zoals bijvoorbeeld:
- een waarschuwing aan betrokkene;
 - melding van de overtreding aan:
 - het voltallige bestuur;
 - de benoemende organisatie met een aanbeveling ten aanzien van eventuele daaraan te verbinden gevolgen (het uiterste gevolg kan zijn dat de benoemende organisatie betrokkene terugtrekt uit het bestuur);
 - de Nederlandsche Bank of de Autoriteit Financiële Markten;
 - ontslag door het bestuur uit de functie.

Het voorgaande laat onverlet een vordering tot schadevergoeding en/of aangifte bij de justitiële autoriteiten.

Artikel 10 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 bindende uitspraak 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.

Artikel 11 Onvoorziene omstandigheden

Voor kwesties waarin deze gedragscode niet voorziet, beslist het dagelijks bestuur van VLEP.

Artikel 12 Slotbepalingen

- 12.1** Het bestuur kan de gedragscode te allen tijde wijzigen.
- 12.2** Naast deze gedragscode beschikt VLEP over een incidenten- en klokkenluidersregeling.
- 12.3** De onderhavige gedragscode is door het bestuur vastgesteld op 1 oktober 2026 en vervangt alle vorige gedragscodes.

Bijlage 1

REGELING GEBRUIK PENSIOENFONDSEIGENDOMMEN

Gebruik iPad

VLEP vergadert papierloos en geeft in verband hiermee respectievelijk een iPad-Pro of een iPad in bruikleen aan ieder lid van het bestuur en het verantwoordingsorgaan van VLEP (hierna: gebruiker) onder de in deze regeling genoemde voorwaarden. Indien een lid van het bestuur of verantwoordingsorgaan geen iPad-pro of iPad in bruikleen heeft gekregen van VLEP is deze regeling niet van toepassing.

Rechten en plichten gebruiker

1. VLEP verstrekt aan gebruiker in bruikleen een iPad van het merk Apple met iPad Case beschermhoes en overige toebehoren (lader e.d.) ten behoeve van papierloos vergaderen door het bestuur van VLEP. De iPad of iPad-Pro is en blijft eigendom van VLEP.
2. Gebruiker verklaart de iPad of iPad-Pro in goede staat te hebben ontvangen. Gebruiker is verantwoordelijk voor het in goede en representatieve staat houden van de iPad of iPad-Pro .

Gebruik

3. VLEP gebruikt de iPad of iPad-Pro ten behoeve van het papierloos vergaderen. Het is gebruiker toegestaan de iPad of iPad-Pro voor overige activiteiten te gebruiken zolang deze activiteiten niet in strijd zijn met de bepalingen in deze regeling gebruik pensioenfondseigendommen.
4. De afschrijftermijn van de iPad-Pro is vier jaar. De afschrijftermijn van de iPad is 3 jaar. Het dagelijks bestuur besluit of de iPad-Pro en iPad na de periode van afschrijving het eigendom van de leden van het bestuur en het verantwoordingsorgaan worden, dit gebeurt niet automatisch nadat de termijn van afschrijving is afgelopen.

Termijn van gebruik

5. Gebruiker dient de iPad of iPad-Pro bij beëindiging van zijn/haar functie binnen het bestuur van VLEP in goede staat te retourneren bij het bestuurssecretariaat. Indien gebruiker niet aan deze verplichting voldoet, dan verbindt gebruiker zich tot betaling van de vervangingswaarde van de apparatuur aan VLEP.
6. Het dagelijks bestuur kan beslissen dat een voormalig lid van het bestuur of het verantwoordingsorgaan de iPad of iPad-Pro niet hoeft te retourneren aan VLEP en het eigendom wordt van het voormalig lid van het bestuur of het verantwoordingsorgaan.

Diefstal en beschadiging

7. Gebruiker dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de iPad of iPad-Pro .

In geval van schade of diefstal van de iPad of iPad-Pro is Gebruiker verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij het bestuurssecretariaat van VLEP en bij de voorzitter van het bestuur te melden.

Bij verlies of diefstal moet dit worden aangegeven bij de politie. Een kopie van deze aangifte dient te worden ingeleverd bij het bestuurssecretariaat van VLEP.

Gebruiker kan aansprakelijk worden gesteld voor schade aan de iPad ontstaan door verwijtbare nalatigheid of onachtzaamheid. Bij vervanging van de iPad door onzorgvuldig handelen worden de kosten voor herstel doorberekend aan gebruiker.

Gedragsregels

8. De via de iPad of iPad-Pro door VLEP beschikbaar gestelde informatie is strikt vertrouwelijk en dient als zodanig te worden behandeld. VLEP kan niet aansprakelijk worden gesteld voor (financiële) schade veroorzaakt door onzorgvuldig gebruik van de informatie op de iPad of iPad-Pro.

Gebruiker dient de iPad of iPad-Pro met een wachtwoord te beveiligen om te voorkomen dat anderen toegang krijgen tot informatie op de iPad of iPad-Pro .

Deze gedragsregels gelden ook voor het gebruik van het bestuurdersportaal.

Slotbepaling

9. VLEP behoudt zich het recht voor om de bruikleen zonder opgaaf van reden in te trekken.



Gedragsrichtlijn “Veilig en bewust digitaal werken” VLEP



pensioenfonds **VLEP**

Documentmanagement

Inwerkingtreding

Deze gedragsrichtlijn is door het bestuur vastgesteld tijdens de bestuursvergadering van 30 januari 2025 en treedt per deze datum in werking.

Evaluatie

Dit document wordt jaarlijks herijkt en vastgesteld. Indien daartoe aanleiding is (zoals bijvoorbeeld in het geval van relevante organisatorische wijzigingen, uitkomsten risicoanalyses en/of wijziging van wet- en regelgeving) kan worden besloten tot tussentijdse herziening.

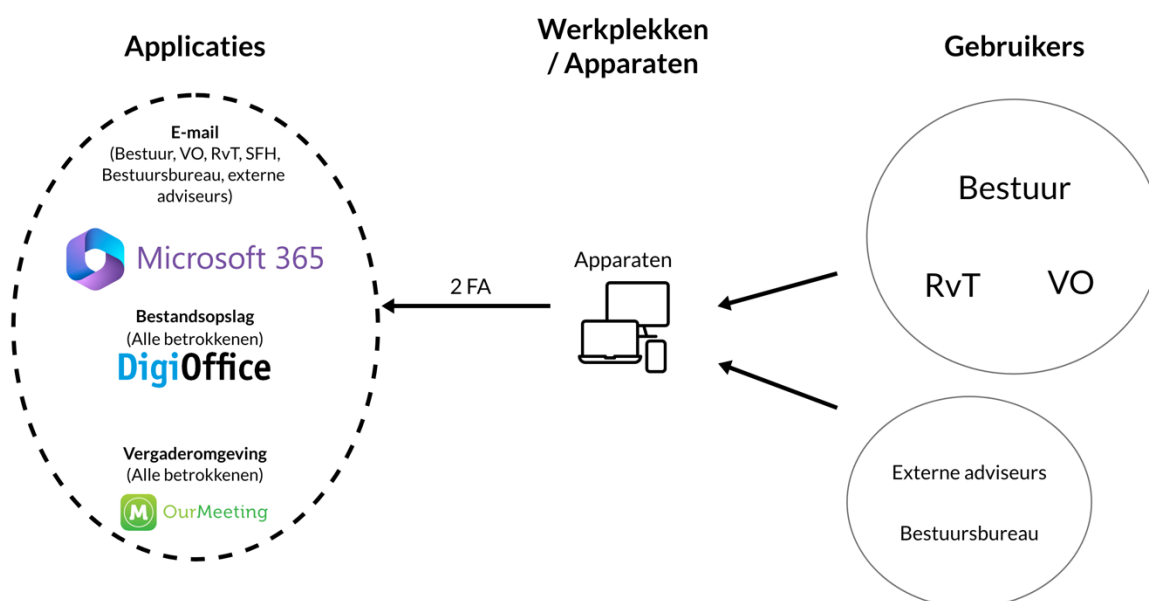
Versiebeheer

Versie	Auteur	Datum	Revisie
0.1	Kouters Van der Meer	18-10-2023	Opstellen conceptversie
0.2	Kouters Van der Meer	28-11-2023	Opstellen concept voor bespreking door bestuur
0.3	Kouters Van der Meer	20-01-2025	Verwerken aanvullende DORA-vereisten
0.4	Actor bureau voor sectoradvies	30-1-2025	Aanpassing naar aanleiding bestuursvergadering 30-1-2025
1.0	Actor bureau voor sectoradvies	30-1-2025	Vastgesteld door bestuur 30-1-2025

1. Inleiding

Binnen de Bestuursomgeving van Stichting Bedrijfstakpensioenfonds voor Vlees, Vleeswaren, Gemaksvoeding en Pluimveevlees (hierna ‘VLEP’) wordt door gebruikers gebruik gemaakt van apparaten en applicaties voor het opslaan, delen en bewerken van bestanden en gegevens van het fonds. Hierdoor is het niveau van informatiebeveiliging dat het fonds nastreeft mede afhankelijk van de beveiliging van deze apparaten en applicaties.

In deze Gedragsrichtlijn “Veilig en bewust digitaal werken” (hierna: ‘deze gedragsrichtlijn’) beschrijft het fonds de voorwaarden die worden gesteld aan het gebruik én de beveiliging van deze apparaten en applicaties, alsook aan de opslag en omgang met (vertrouwelijke) informatie van het fonds. Deze voorwaarden zijn erop gericht een gewenst minimaal beveiligingsniveau te realiseren. Dit betreft niet alleen technische instellingen, maar ook de wijze waarop gebruikers omgaan met informatie van het fonds en de apparaten en applicaties die zij gebruiken ten behoeve van de uitvoering van de functie voor het fonds.



Figuur 1: Bestuursomgeving van het fonds

1.1. Reikwijdte

Deze gedragsrichtlijn is van toepassing op de bestuursomgeving van het fonds. Hiertoe behoren de volgende onderdelen:

- **Gebruikers:** iedereen die gebruik maakt van gegevens van het fonds. Deze gedragsrichtlijn richt zich specifiek tot de aan het fonds verbonden personen (bestuursleden, verantwoordingsorgaan (VO), Raad van Toezicht (RvT), sleutelfunctiehouders, privacy officer, compliance officer), bestuursbureau, en externe verbonden personen (o.a. adviseurs):
 - **Gebruikers met een Microsoft 365 account van het fonds:** gebruikers die een eigen Microsoft 365 account van het fonds hebben en daarmee onderdeel zijn van de autorisatiestructuur en role-based access hebben tot fondsgegevens in Microsoft 365.
 - **Gebruikers zonder een Microsoft 365 account van het fonds:** gebruikers die geen eigen Microsoft 365 account van het fonds hebben. Fondsgegevens worden, indien nodig, op bestandsniveau gedeeld met de betreffende gebruiker.
- **Apparaten:** smartphones, tablets, laptops. Apparaten worden onderverdeeld in de volgende twee categorieën:
 - **Fonds apparaten:** een apparaat uitgegeven door het fonds.
 - **Persoonlijke apparaten:** een privé apparaat dat voor zakelijke doeleinden (t.b.v. het fonds) gebruikt wordt.
- **Applicaties:** Microsoft 365, OurMeeting en DigiOffice.

2. Uitgangspunten

De uitgangspunten geven uiting aan de speerpunten voor het fonds ten aanzien van informatiebeveiliging binnen de bestuursomgeving. De uitgangspunten zijn hoofdzakelijk onder te verdelen in twee categorieën: Informatiebeveiliging ten gevolge van het *gedrag* van gebruikers, en informatiebeveiliging ten gevolge van het hanteren van de juiste *technische instellingen* (security baselines) door gebruikers. Hier geven respectievelijk hoofdstuk 3 en hoofdstuk 4 nadere invulling aan.

2.1. Praktisch en Pragmatisch

Gezien de omvang en samenstelling van de organisatie van het fonds zijn praktische maatregelen belangrijker dan theoretische verhandelingen. Bij het definiëren van maatregelen wordt het beginsel van proportionaliteit in acht genomen.

2.2. Verantwoordelijkheid voor individuele gebruikers

Veilig werken binnen de bestuursomgeving begint bij het nemen van verantwoordelijkheid door de individuele gebruikers. Bij alle gebruikers binnen het fonds staat professionaliteit, vertrouwelijkheid en integriteit voorop. Bovendien is informatiebeveiliging een zaak van iedereen. De gebruiker is verantwoordelijk voor veilig gebruik van het apparaat, applicaties en Microsoft 365 en daarmee voor de naleving van de uitgangspunten, basisregels en security baselines zoals opgenomen in deze beleidsrichtlijn.

2.3. Hoge mate van bewustzijn en focus op preventie

De gebruiker vormt een risico voor informatiebeveiliging, maar is ook de ‘first line of defense’. Daarom streeft het fonds naar een hoge mate van bewustwording van het thema informatiebeveiliging bij gebruikers binnen de bestuursomgeving. Daarnaast geldt het uitgangspunt dat zoveel als mogelijk preventieve maatregelen zijn getroffen om de risico’s bij gebruik van IT-middelen, zowel apparaten als applicaties, te beperken.

3. Basisregels

De basisregels richten zich op het gebruik, het beheer en de beveiliging van de digitale bestuursomgeving. Hiermee wordt bijgedragen aan het bewustzijn van gebruikers met betrekking tot het veilig omgaan met apparaten, applicaties, en de gegevens die zich hierin bevinden en de gebruiker inziet, bewerkt en opslaat. Gezien de meeste basisregels niet gecontroleerd kunnen worden, steunt het fonds op uitgangspunt 2.2 “verantwoordelijkheid van individuele gebruikers” ten aanzien van het toepassen van de basisregels.

Fondsgegevens die worden opgeslagen, overgedragen of verwerkt op mobiele apparaten zijn en blijven eigendom van het fonds, tezamen met de applicaties en databases betrekking hebbende op de bestuurlijke IT-werkomgeving van het fonds waartoe zij toegang hebben met hun eigen apparaten (bijvoorbeeld door middel van lokaal geïnstalleerde apps). Apparaten en applicaties zijn ‘entry points’ tot fondsgegevens en dienen daarom adequaat beheerd te worden door gebruikers.

Bestuursleden en interne toezichthouders (RvT, VO) ondertekenen voorafgaand aan het gebruik van apparaten de gebruikers-verklaring (zie bijlage 1).

Gebruikers waarmee dienstverleningsafspraken gemaakt zijn (bestuursbureau, externe adviseurs) nemen kennis van deze beleidsrichtlijn bij het aangaan van



dienstverleningsafspraken en bevestigen zich aan deze beleidsrichtlijn te houden en aan de security baseline te voldoen.

Gebruikers zorgen dat fondsgegevens van het apparaat verwijderd zijn indien zij het apparaat vernietigen, weggeven, verkopen of op een andere manier niet meer in bezit houden. Bijvoorbeeld door het apparaat terug te zetten naar fabrieksinstellingen.

Het mobiele apparaat wordt uitsluitend gebruikt door de gebruiker die het apparaat bij het fonds heeft geregistreerd. Bij gebruik door naasten treft de eigenaar gepaste (beveiligings)maatregelen.

Nadat een gebruiker uit dienst treedt, worden de fondsapparaten die gebruikt werden door de betreffende gebruiker (zie sectie 1.1) ingeleverd bij het fonds.

Gebruikers krijgen toegang tot de digitale bestuursomgeving via unieke accounts die worden gecreëerd bij indiensttreding. De (fysieke) toegangsrechten van gebruikers worden bepaald op basis van de 'need-to-know', 'need-to-use'- en 'least privilege'-principes en op basis van functiescheiding. De rechten worden gewijzigd of geüpdatet wanneer hier aanleiding toe is en deze aanpassingen in lijn zijn met de functie(wijziging) van de gebruiker. Accounts worden jaarlijks gereviewd om te controleren of de rechten nog passend zijn en de gebruiker van het account nog in dienst is. Unieke accounts worden verwijderd wanneer de gebruiker niet meer in dienst is.

De rechten binnen kritieke systemen en binnen kritieke en belangrijke (KOB) systemen worden halfjaarlijks gereviewd. De rechten van niet-kritieke systemen worden jaarlijks gereviewd.

Niet-persoonsgebonden accounts worden zo min mogelijk gebruikt en zo veel mogelijk beperkt in toegangsrechten, tenzij dit niet anders mogelijk is. Toegang tot niet-persoonsgebonden accounts wordt gemonitord. Nood- en administrator rechten worden alleen gebruikt wanneer dit nodig en verantwoord is en noodrechten worden direct na de crisissituatie ingetrokken.

4. Do's en Dont's

DO

Fondsgegevens/ apparaten

Sla, indien dit noodzakelijk is, bestanden in de 'lokale' OneDrive op, waarbij sprake is van automatische synchronisatie om gegevensverlies te voorkomen.

Toegangsbeveiliging

Gebruik door het fonds uitgegeven apparaten uitsluitend voor werkzaamheden ten behoeve van het fonds.

Zorg, bij gebruik van apparaten op openbare plaatsen, dat niet kan worden meegelezen door onbevoegde personen. Bijvoorbeeld middels een privacy screen voor laptops.

Gebruik voor elk account een uniek wachtwoord. Wanneer een wachtwoord is gelekt in een datalek, is de kans namelijk groot dat een hacker dit wachtwoord probeert om andere accounts binnen te dringen.

DON'T

Fondsgegevens/ apparaten

Download fondsgegevens niet naar het apparaat.

Print fondsdocumentatie niet. Indien het noodzakelijk is om documenten te printen dient hier verantwoordelijk mee omgegaan te worden en in het geval van gevoelige documenten veilig vernietigd te worden.

Het is verboden om illegale software (software zonder geldige licentie) op mobiele apparaten te installeren. Tevens is het verboden om illegale media (waaronder films, series, muziek en E-books) te downloaden en op mobiele apparaten op te slaan.

Toegangsbeveiliging

Installeer geen Apps die niet afkomstig zijn vanuit de App store of waarvan de ontwikkelaar en/of aanbieder van de app onbetrouwbaar is. De betrouwbaarheid kan bijvoorbeeld worden gecontroleerd via google of op consumentenwebsites.

Laat apparaten niet onbeheerd achter, met uitzondering van de huiselijke omgeving en de beveiligde kantooromgeving.

Schrijf wachtwoorden niet op en deel wachtwoorden niet met anderen. Gebruik voor het onthouden van wachtwoorden een wachtwoordmanager.

Gebruik bij voorkeur een wachtwoordmanager voor het genereren en opslaan van sterke wachtwoorden.

Maak, voor zover mogelijk, gebruik van multi-factor authenticatie bij accounts. Dit is een additionele beveiligingsstap in het geval de hacker het wachtwoord heeft achterhaald.

Gebruik van internet en e-mail

Maak bij voorkeur gebruik van bekende en beveiligde (Wi-Fi) netwerken.

Meld verdachte (phishing) e-mails of berichten gerelateerd aan inboxen, apparaten en accounts van het fonds terstond bij het Bestuursbureau. Op deze manier kan uitgezocht worden of het daadwerkelijk een phishing mail is, en kunnen andere gebruikers gewaarschuwd worden.

Meld terstond bij het Bestuursbureau indien op een (potentiële) phishing mail is geklikt. Ook al is dit niet leuk om te doen, het is belangrijk dat eventuele schade direct beperkt wordt.

Verander je wachtwoord indien je vermoed gehackt te zijn, of als het wachtwoord in een datalek is gedetecteerd (wachtwoordmanagers controleren hierop en signaleren indien een gebruikt wachtwoord in een datalek is gevonden).

Deel documenten via een beveiligde transfer-methode.

Vermijd kenmerkende gegevens in wachtwoorden (geboortedata, namen, adresgegevens). Hackers kunnen een wachtwoord anders gemakkelijk raden.

Gebruik van internet en e-mail

Maak geen connectie met openbare Wi-Fi netwerken. Maak gebruik van een passend alternatief, zoals een VPN-verbinding of de hotspot van de smartphone, indien een bekende en beveiligde verbinding niet beschikbaar is.

Schakel het automatische forwarden van mailberichten uit. *N.B. Met forwarding wordt bedoeld; automatisch doorsturen naar andere (externe) e-mailadressen.*

Deel vertrouwelijke gegevens en persoonsgegevens niet per e-mail en sla deze ook niet op buiten de bestuurlijke werkomgeving, tenzij dit noodzakelijk is. Gebruik OurMeeting voor het delen van informatie of een beveiligde transfer-methode (SharePoint) als OurMeeting niet mogelijk is.

5. Security baselines

Ter bevordering van de pragmatische implementatie van deze richtlijn is een security baseline opgesteld. De security baseline functioneert als een checklist per type apparaat voor het controleren van de (beveiligings)instellingen van mobiele apparaten. Wanneer een gebruiker niet aan een instelling kan voldoen is het van belang dat het minimale informatiebeveiligingsniveau geborgd blijft door additionele maatregelen te nemen.

Instelling	Van toepassing bij desktop/ laptop	Van toepassing bij Smartphone/ tablet	Van toepassing bij applicaties
Apparaten beschikken over een iOS (Apple), Android (Google), WindowsOS (Microsoft) of MacOS (Apple) besturingssysteem. Het is verboden om gebruik te maken van 'Jailbreaking' (Apple), 'Rooting' (Google) of andere methoden die de integriteit van het besturingssysteem compromitteren.	Ja WindowsOS (Microsoft), MacOS (Apple) of Android (Google).	Ja iOS (Apple) of Android (Google).	n.v.t.
Apparaten en daarop gebruikte software worden actief ondersteund door beveiligings-updates. Nieuwe updates van het besturingssysteem worden automatisch geïnstalleerd.	Ja	Ja	Ja
De harde schijf van (nieuwe) apparaten is versleuteld.	Ja	n.v.t.	n.v.t.

Instelling	Van toepassing bij desktop/ laptop	Van toepassing bij Smartphone/ tablet	Van toepassing bij applicaties
Automatische vergrendeling van het scherm na inactiviteit.	5 minuten	Smartphone: 1 minuut Tablet: 5 minuten	n.v.t.
Apparaten en accounts zijn beveiligd middels sterke authenticatiemethodes, wanneer van toepassing in overeenstemming met specifieke systeemclassificaties.	Ja Tenminste één van de volgende opties: <ul style="list-style-type: none"> - >12 karakters, opgebouwd uit een combinatie van letters, hoofdletters, cijfers en bijzondere tekens. - Vingerafdruk-scanner - Gezichts-herkenning 	Ja Tenminste één van de volgende opties: <ul style="list-style-type: none"> - >6 karakters - Vingerafdruk-scanner - Gezichts-herkenning 	Ja >12 karakters, opgebouwd uit een combinatie van letters, hoofdletters, cijfers en bijzondere tekens
Accounts zijn beveiligd middels 2-Factor authenticatie (2FA).	n.v.t.	n.v.t.	Ja
Gegevens worden gewist na 10 verkeerde inlogpogingen.	n.v.t.	Ja	n.v.t.
'Find My' (Apple), 'Find My Device' (Google) of 'Mijn apparaat zoeken' (Windows) functionaliteit is ingeschakeld	Ja	Ja	n.v.t.
Apparaten worden regelmatig (automatisch) gescand op bedreigingen door middel van gerenommeerde antivirussoftware ³ .	Ja	Ja	n.v.t.
De ingebouwde firewall van het besturingssysteem is ingeschakeld.	Ja	n.v.t.	n.v.t.