Stichting De Samenwerking
Pensioenfonds voor het
Slagersbedrijf

**10-4-2018**

# Pensioenfonds voor het Slagersbedrijf

# IT beleid 2018

# Versie 1.0

**DOCUMENTMANAGEMENT**

### Versiebeheer

Voor u ligt het concept IT beleid van Pensioenfonds voor het Slagerspensioenfonds (BPS).

### Distributie

| Datum | Naam | Opmerking |
|---|---|---|
| 29 maart 2017 | Bestuur BPS en Sprenkels & Verschuren | Bespreking Uitgangspunten IT-beleid |
| 19 april 2017 | IRM-Commissie BPS | Vervolg bespreken Uitgangspunten IT-beleid |
| 12 oktober 2017 | Bestuur BPS en Sprenkels & Verschuren | Bespreking IT-beleid algemeen |
| 1 november 2017 | IRM-Commissie BPS | Bespreking eerste concept IT Beleid |
| 1 februari 2018 | IRM-commissie BPS | Bespreking tweede concept IT Beleid |
| 12 maart 2018 | IRM-commissie BPS | Definitief concept IT beleid voor verzending naar bestuur BPS |
| 10 april 2018 | Bestuur BPS | Formeel akkoord bestuursleden en vaststelling van het IT Beleid |

# 1. INLEIDING

Pensioenfondsen waarop artikel 143 van de Pensioenwet van toepassing is, dienen ingevolge het eerste lid van dat artikel hun organisatie zodanig in te richten dat deze een beheerste en integere bedrijfsvoering waarborgt. Dit brengt met zich mee dat deze instellingen voor zover van toepassing – dat wil zeggen proportioneel toegepast - dienen te beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen. Daarnaast dient een pensioenfonds te voldoen aan artikel 13 Wet bescherming persoonsgegevens, waarin is geregeld dat er passende technische en organisatorische maatregelen ten uitvoer moeten worden gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Vanaf invoering van Algemene verordening gegevensbescherming(AVG) per 25 mei 2018 dient een pensioenfonds daarnaast te voldoen aan artikel 24 en 32 van die verordening, waarin is geregeld dat er passende technische en organisatorische beveiligingsmaatregelen zijn getroffen tegen onrechtmatige verwerking, verlies, vernietiging en beschadiging van persoonsgegevens.

# 2. DOEL EN TOEPASSELIJKHEID

Het Pensioenfonds voor het Slagersbedrijf (hierna: BPS) kan binnen het werkterrein waarin zij actief is niet zonder IT-inzet. Het gebruik van Informatietechnologie (IT) is essentieel voor de realisatie van de strategische doelen van BPS. IT richt zich daarbij op het verschaffen van juiste, volledige, vertrouwelijk relevante en tijdige informatieverstrekking, zowel intern (bestuur, commissies, toezichthouder, verantwoordingsorgaan en bestuursbureau) als extern (stakeholders, externe toezichthouders).
IT raakt alle fondsprocessen en is daarmee veelomvattend en complex. In het IT-beleid worden onder andere de volgende onderdelen onderkend en beschreven:
- IT als essentieel instrument voor BPS;
- waarborgen rondom IT-processen en IT-uitgangspunten;
- samenhang fondsstrategie, risicohouding en IT;
- IT-risico's en risicoanalyse, risicobeheersing en maatregelen;
- uitbesteding van IT-processen, toetsing en monitoring.

Risicobeheersing neemt een belangrijke plaats in het IT-beleid in. Het IT-risico moet passen binnen de risicobereidheid van BPS. Deze risicobereidheid is afgeleid van de missie, visie, kernwaarden en strategie van BPS. Op basis hiervan zijn de uitgangspunten IT-Beleid geformuleerd. In de volgende paragrafen wordt dit verder uitgewerkt.

# 3. BIJSTELLING IT BELEID

- Dit IT-beleid is door het bestuur van BPS goedgekeurd op 10 april 2018.
- Tenminste één keer per jaar wordt nagegaan of bijstelling van het IT beleid noodzakelijk is.

# 4. WETTELIJK KADER

Conform de Wet Financieel Toezicht, de Algemene verordening gegevensbescherming(AVG) en de Pensioenwet dienen financiële instellingen te beschikken over adequate procedures en maatregelen ter beheersing van de IT-risico's. Het gaat hierbij onder meer om het waarborgen van de continuïteit van de IT en de beveiliging van informatie. Adequaat betekent in dit verband dat de procedures zijn gebaseerd op de aard van de financiële instelling en de complexiteit van de organisatie. De procedures moeten voldoen aan algemeen geaccepteerde standaarden (good practices). Ook dienen

ze bij voorkeur afgestemd te zijn op de bedrijfstak-specifieke omstandigheden van de desbetreffende financiële instelling. Een voorbeeld van dergelijke standaarden zijn Cobit en ISO27000. Deze standaarden bevatten in beginsel door DNB toereikend geachte maatregelen.
Specifiek voor het waarborgen van de beveiliging van informatie heeft DNB een toetsingskader gemaakt bestaande uit een selectie van Cobit. Instellingen dienen hierbij voor alle maatregelen te voldoen aan een volwassenheidsniveau van minimaal 3 (“aantoonbare werking”). In 2014 is het toetsingskader geactualiseerd en geldt voor drie maatregelen uit de categorie "Assess and manage (IT) risks" per 1 juni 2015 een minimaal volwassenheidsniveau van 4. Deze aanpassingen staan beschreven in het document 'Toelichting op Toetsingskader 2014' (www.toezicht.dnb.nl.binaries/50-230767.pdf).

Pensioenfondsen en beroepspensioenfondsen waarop artikel 143 van de Pensioenwet (PW) onderscheidenlijk artikel 138 van de Wet verplichte beroepspensioenregeling van toepassing is, dienen ingevolge het eerste lid van die beide artikelen hun organisatie zodanig in te richten dat deze een beheerste en integere bedrijfsvoering waarborgt. In het tweede lid van deze artikelen, aanhef en onderdeel a, is bepaald dat bij of krachtens algemene maatregel van bestuur regels worden gesteld met betrekking tot het eerste lid van die artikelen wat betreft het beheersen van bedrijfsprocessen en bedrijfsrisico's.
Van een nadere uitwerking van het vereiste van een beheerste en integere bedrijfsvoering in regels met betrekking tot het beheersen van bedrijfsprocessen en bedrijfsrisico's overeenkomstig het bepaalde in artikel 20, tweede lid Bpr, is voor pensioenfondsen en beroepspensioenfondsen geen sprake, anders dan dat zij beschikken over goede administratieve en boekhoudkundige procedures en adequate interne controlemechanismen en beleid ten aanzien van de beheersing van de te lopen risico's (artikel 18 van het Besluit financieel toetsingskader pensioenfondsen).

Dit laat onverlet dat DNB van oordeel is dat de overeenkomstige toepasselijkheid voor deze (beroeps)pensioenfondsen van de algemene norm inzake een zodanige organisatie-inrichting dat deze een beheerste en integere bedrijfsvoering waarborgt, met zich brengt dat ook deze instellingen voor zover van toepassing – dat wil zeggen proportioneel toegepast - dienen te beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen.

Vorig jaar heeft DNB in dit kader bij een aantal pensioenfondsen een self assessment uitgevoerd en aanvullende gesprekken gevoerd. In het verlengde van dit onderzoek heeft de Pensioenfederatie een service document ICT opgesteld. Deze is als leidraad gebruikt voor het opstellen van dit IT-beleid.

## 5. Comply or Explan principe

De naleving van het IT beleid vindt plaats volgens het ‘comply or explain’ oftewel ‘voldoen of verklaar’ beginsel. Dit betekent dat BPS wel kan samenwerken met uitbestedingspartijen die afwijken van dit beleid, mits die partijen daar een aanvaardbare en bij behorende reden voor hebben. Het eventuele afwijkende beleid dient wel te passen bij de risicohouding en risicobeheersing van het fonds. Dit zal dan besproken moeten zijn met het bestuur.

## 6. Relaties en referentie

Bij het opstellen van dit document zijn de volgende richtlijnen en beheersmaatregelen meegenomen:

- Gedragscode en naleving (door interne compliance officer)
- ISO 27001/2
- CoBiT model
- DNB FIRM & FOCUS model

- COSO - Enterprise Risk Management (ERM) model

## 7. IT RISICOANALYSE

Op basis van een risicoanalyse wordt het gewenste niveau van beheersing bepaald door het Bestuur. Daarbij wordt o.a. gekeken naar de volgende drie aspecten: **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid. De zogenaamde BIV classificatie. De genoemde aspecten worden binnen het vakgebied informatiebeveiliging als volgt gedefinieerd:

*Beschikbaarheid*
Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen). Zodat het Bestuur en de deelnemers van het fonds gewaarborgd zijn van continuïteit.

*Integriteit*
Integriteit betreft het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan. Zodat het Bestuur en de deelnemers van het fonds gewaarborgd zijn van continuïteit en het Bestuur op een integere wijze besluitvorming kan realiseren.

*Vertrouwelijkheid*
Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Zodat het Bestuur en de deelnemers van het fonds gewaarborgd zijn van continuïteit en dat er ook geen compliance issues zijn die een reputatie- en/of financiële schade kunnen veroorzaken.

## 8. IT RISICO'S

IT-risico's zijn risico's die verband houden met het onvoldoende (of niet continu) beveiligd zijn van bedrijfsprocessen en onbetrouwbare informatievoorziening. Deze risico's kunnen zich voordoen als bijvoorbeeld de IT-strategie en het IT-beleid niet of onvoldoende zijn toegesneden op de bedrijfsprocessen. IT-risico's kunnen optreden bij:

- de beveiliging (bijvoorbeeld toegang voor niet-geautoriseerde gebruikers tot vertrouwelijke informatie);
- de beheersbaarheid (onvoldoende beheer van de IT-omgeving); en
- juistheid, betrouwbaarheid en continuïteit.

Ten aanzien van de IT zijn de volgende risico's benoemd:

**A. ICT: MENSELIJKE RISICO'S**
A1 Mutaties in personeelsbestand
A2 Bedienings- / gebruikersfout
A3 Lekken
A4 Onderhoudsfout aan netwerk, software en/of hardware
A5 Capaciteitstekort
A6 Besluitvormingstekortkomingen
A7 Diefstal, ontvreemding en/of misbruik door buitenstaanders
A8 Diefstal, ontvreemding en/of misbruik door insiders
A9 Interne fraude
A10 Externe fraude

**B. ICT: TECHNOLOGISCHE RISICO'S**
B1 Technische storing aan netwerk
B2 Technische storing aan randapparatuur
B3 Storingen in software en interfaces
B4 Technische tekortkomingen database
B5 Storingen in overige apparatuur

**C. ICT: OMGEVINGSRISICO'S**
C1 Omgevingsveranderingen
C2 Natuurrampen/-incidenten (calamiteiten)
C3 Terrorisme en Sabotage
C4 Cyberaanval en Spionage
C5 Tekortschietende alignment

## 9. UITGANGSPUNTEN IT-BELEID

BPS stelt het IT beleid periodiek vast aan de hand van de missie, visie, strategie en de risicohouding en risicobereidheid. De kernwaarden zijn: 1. Betrouwbaar 2. Transparant 3. Betrokken 4. Deskundig 5. Bereikbaar en 6. Duurzaam. Het IT beleid past binnen deze kernwaarden.
Het IT-beleid draagt bij aan de kerntaak van het pensioenfonds. De uitgangspunten van het IT beleid passen binnen deze kernwaarden en staan hiermee niet op zichzelf.

*Betrouwbaar*
De kernwaarde 'betrouwbaar' komt tot uitdrukking in de eis van het Bestuur om datalekken te voorkomen. Uitvoerders moeten tijdig en proactief informatie delen, bijvoorbeeld ten aanzien van incidenten. Het Bestuur is en blijft eigenaar van alle data en werkt alleen met innovatieve betrouwbare systemen (fast follower). Bestuursleden werken uitsluitend met beveiligde emailadressen en beveiligde 'own devices'. Medewerkers van uitbestedingspartijen hebben geen toegang tot data, tenzij expliciet toestemming hiervoor is verleend. Het Bestuur wenst door deelnemers te worden gezien als betrouwbaar doordat data niet zonder expliciete toestemming wordt overgedragen aan derden en privé informatie daardoor veilig is opgeslagen en veilig wordt gedeeld. Reputatieschade door toedoen van IT en IT processen moet worden voorkomen.

*Transparant*
De kernwaarde 'transparant' ten aanzien van IT-beleid komt tot uitdrukking in de eis van het Bestuur om juiste, volledige en tijdige informatie te verstrekken aan derden en data integriteit te behouden. Dit aan de ene kant zodat het Bestuur op een integere wijze een besluit kan (laten) nemen en aan de andere kant ook transparantie eist indien er data in de cloud opgeslagen is (wordt). Het Bestuur wenst vooraf geïnformeerd te worden door uitbestedingspartijen.

*Betrokken*
De kernwaarde 'betrokken' komt tot uitdrukking in de wens van het Bestuur om voldoende inzicht te verkrijgen en te houden in de IT (uitbestedings)keten. Het Bestuur is zich bewust van de eigen verantwoordelijkheid ook al zijn bepaalde werkzaamheden uitbesteed aan andere partijen. Non-compliancy ten aanzien van IT moet worden voorkomen. Het Bestuur zelf heeft een interne verantwoordelijkheid als het gaat om dataopslag op privé PC's (thuis) en/of op ipads en andere mobiele devices.

*Deskundig*
De kernwaarde 'deskundig' komt tot uitdrukking in de wens van het Bestuur om IT kennis aan de bestuurstafel te hebben. IT kennis kan hierdoor worden gedeeld met de overige bestuursleden, waardoor alle bestuursleden, het effect van IT op processen en beleid begrijpen. De uitvoerders moeten ook over voldoende kennis beschikken ten aanzien van de applicaties waarop BPS (data) draait (ook bij End User Computing). Het Bestuur wil IT begrijpelijk houden en niet complexer maken dan noodzakelijk. Dit komt ook tot uiting in het IT landschap en de taal die gebruikt (moet) worden

*Bereikbaar*
De kernwaarde 'bereikbaar' komt tot uitdrukking in de wens van het Bestuur om waarde creërend te zijn in de communicatie naar de deelnemers en beschikbaarheid op het moment dat een deelnemer het nodig heeft.

*Duurzaam*
De kernwaarde 'duurzaam' komt tot uitdrukking in de wens van het Bestuur om het IT beleid zo in te richten dat het proces goed in balans is (risk en control (IT general controls)) en passend is binnen het totale beleid van BPS. In gevallen van nood moet sprake zijn van uitwijkprocedures, zodat BPS de continuïteit (van de belangen van (gewezen) deelnemers en pensioengerechtigden) zo goed mogelijk kan waarborgen.

## Besturing vanuit het Bestuur
Het initiële aanspreekpunt voor het IT beleid is het bestuur. Daarnaast houdt de IRM-commissie vanuit risicoperspectief bezig met IT -beleid. De governance vanuit het Bestuur is tevens ingesteld op het kunnen bieden van countervailing power aan uitbestedingspartijen. BPS heeft een integere en beheerste bedrijfsvoering voor ogen in doen en handelen.

## Risicohouding en Risicobereidheid van het Bestuur
De risicohouding en de risicobereidheid van BPS is afgeleid van de missie, visie en strategie van BPS, waarbij het fonds telkens de afweging maakt tussen het volgen van de strategie (minimaal voldoen aan wet- en regelgeving) en kosten die behoren bij te nemen beheersmaatregelen. Risicohouding en Risicobereidheid van het bestuur staan geformuleerd in het IRM-Beleidsdocument.

## IT Uitgangspunten van BPS op basis van risicohouding
Het Bestuur van BPS heeft een aantal uitgangspunten van het IT beleid geformuleerd, waaraan zowel de bestuursleden van BPS (intern) als de uitbestedingspartijen (extern) moeten voldoen.

De IT-uitgangspunten luiden als volgt:

1. Het IT-beleid past binnen het totale beleid van het Pensioenfonds voor het Slagersbedrijf (BPS)

2. De beheersing van IT-risico's krijgt de aandacht en tijd die nodig is.

3. BPS vereist van de uitbestedingspartijen een periodieke verklaring ten aanzien van hun bedrijfsvoering naast een ISAE of andere assuranceverklaring.

4. BPS is en blijft eigenaar van alle overdraagbare data. Data wordt niet zonder toestemming vooraf beschikbaar gesteld aan derden.

5. Reputatie- en financiële schade van BPS door toedoen van IT en IT-processen moeten worden voorkomen.

6. Om het IT-beleid goed vorm te kunnen geven en ook overige kennis van IT te borgen en de risico's daaromtrent te kunnen benoemen, staat IT-kennis regelmatig op de bestuurlijke agenda.

7. Data-integriteit wordt behouden of versterkt.

8. Het bestuur heeft inzicht in de IT-(uitbestedings)keten. Onder de IT-(uitbestedings)keten vallen ook de sub-serviceorganisaties van uitvoerders.

9. Het bestuur wenst een "right tot audit" te hebben in de gehele keten van uitbesteding (direct en indeicrect) waarbij het enkel verstrekken van een ISAE 3402 niet voldoende is.

10. Uitbestedingspartijen moeten Business Continuity Management hebben ingericht en ook een Business Impact Analyse hebben uitgevoerd. Dit houdt kort gezegd in dat bij uitvoerders sprake moet zijn van uitwijkprocedures in gevallen van nood.

11. Uitbestedingspartijen dienen in staat te zijn verandertrajecten op gebied van IT te realiseren.

12. De totale kosten van IT in relatie tot de overall kosten moeten inzichtelijk zijn.

**Samenvattend:**
BPS stelt het IT beleid periodiek vast aan de hand van de missie, visie, strategie en de risicohouding en risicobereidheid. De kernwaarden zijn: 1. Betrouwbaar 2. Transparant 3. Betrokken 4. Deskundig 5. Bereikbaar en 6. Duurzaam. Het IT beleid past binnen deze kernwaarden.

Het IT beleid bestaat uit een normenkader (IT Uitgangspunten) waar het Bestuur en de uitbestedingspartijen, (de pensioenadministratie, de beleggingsadministratie, de werkzaamheden inzake actuariële berekeningen en de belegging van het vermogen van het fonds) aan moeten voldoen. De naleving van het IT beleid vindt plaats volgens het 'comply or explain' beginsel. Dit betekent dat BPS wel kan samenwerken met uitbestedingspartijen die afwijken van dit beleid, mits die partijen daar een goede reden voor hebben.