Beleidsdocument Informatiebeveiliging

Stichting Bedrijfstakpensioenfonds
voor de betonproductenindustrie

December 2021

Inhoud

1 Inleiding

Informatiebeveiliging is heden ten dage een van de belangrijkste aandachtspunten voor het Bedrijfstakpensioenfonds voor de Betonproductenindustrie (hierna: Bpf beton) mede in het kader van een beheerste en integere bedrijfsvoering. Derhalve heeft het bestuur beleid over informatiebeveiliging geformuleerd en vastgelegd in het onderhavige beleidsdocument. Dit beleid vormt het uitgangspunt voor de maatregelen die waarborgen dat Bpf Beton en haar uitbestedingsrelaties voldoen aan geldende normen ('best practices') en wet- en regelgeving. Het pensioenfonds blijft te allen tijde verantwoordelijk voor de beheersing van informatiebeveiligingsrisico's, ook voor de uitbestede werkzaamheden.

Informatiebeveiliging draagt bij aan een veilige werkomgeving en schept vertrouwen bij de belanghebbenden van Bpf Beton. Zij mogen er op vertrouwen dat het pensioenfonds informatie beveiligt en dezelfde eisen stelt aan haar uitbestedingsrelaties.

Leeswijzer

Dit document is als volgt opgebouwd. In hoofdstuk 2 wordt de governance beschreven specifiek voor de uitvoering van dit informatiebeveiligingsbeleid. In hoofdstuk 3 is het strategische kader van informatiebeveiliging opgenomen zoals dat door het bestuur in lijn met de missie, visie en strategie is uitgewerkt en vastgesteld. Hoofdstuk 4 beschrijft het inhoudelijke beleid in lijn met de opzet en structuur van het DNB self assessment informatiebeveiliging 2019. Vervolgens beschrijft hoofdstuk 5 de wijze waarop het informatiebeveiligingsbeleid onderdeel is van het integraal risicomanagement en wordt het jaarlijks te doorlopen proces beschreven. In hoofdstuk 6 wordt beschreven dat het bestuur verantwoording aflegt over de uitkomsten van het gevoerde beleid en aan welke partijen. Hoofdstuk 7 beschrijft de periodieke publicatie van het beleid en hoofdstuk 8 wordt tenslotte vermeld wanneer dit beleidsdocument voor het laatst is gewijzigd en vastgesteld.

2 Governance

Dit beleid beschrijft de informatiebeveiliging van Bpf Beton en op wie[1] het van toepassing is.
In beginsel zijn dat het bestuur en de organen van het pensioenfonds (het verantwoordingsorgaan en de raad van toezicht) en alle uitbestedingsrelaties die werkzaam zijn voor het pensioenfonds.

De uitvoering van het informatiebeveiligingsbeleid heeft het bestuur neergelegd bij de IRM-commissie onder voorzitterschap van de sleutelfunctiehouder risicomanagement. Jaarlijks beoordeelt de IRM-commissie of het informatiebeveiligingsbeleid (fonds breed) nog adequaat is respectievelijk aanpassing vergt. Tevens voert de IRM-commissie periodiek een risicoanalyse uit. De uitkomst van de risicobeoordeling wordt met het bestuur gedeeld evenals voorgestelde beleidsaanpassingen.

Kennis van informatiebeveiliging binnen het bestuur is belangrijk. Periodiek beoordeelt het bestuur of er voldoende kennis binnen het bestuur aanwezig is om de risico's goed in te schatten en om voldoende 'countervailing power' te leveren tegenover de uitbestedingspartners van het fonds. De sleutelfunctiehouder risicomanagement is binnen het bestuur het eerste aanspreekpunt voor informatiebeveiliging. Het bestuur is zich er van bewust dat specialistische kennis van tijd tot tijd nodig zou kunnen zijn en zal deze specialistische kennis zo nodig extern inhuren.
Het pensioenfonds heeft de voornaamste processen uitbesteed aan externe partijen. Het pensioenfonds hanteert als voorwaarde voor uitbestedingsrelaties dat zij voldoen aan het informatiebeveiligingsbeleid van het fonds en beschikken over eigen beleid dat minimaal gelijkwaardig is aan het beleid dat Bpf Beton hanteert.
Bpf Beton evalueert periodiek, indien daartoe aanleiding bestaat, of de uitbestedingsrelaties voldoen aan de regels van dit informatiebeveiligingsbeleid. Een audit kan onderdeel gaan uitmaken van de monitoring. Bpf Beton zal tenminste toetsen of de uitbestedingspartij voldoet aan de gestelde eisen van het DNB self-assessment Informatiebeveiliging 2019[2].

Bpf Beton heeft de primaire werkzaamheden uitbesteed aan externe partijen. Het bestuur houdt bij de aangestelde uitbestedingspartijen zicht op de strategische (wijzigingen in) IT-infrastructuur, de IT-processen, dataverwerking, -opslag en -beveiliging en beoordeelt tevens of de uitbestedingspartij voldoet aan de geldende wet- en regelgeving.

Het bestuur meldt 'belangrijke of kritieke activiteiten' van een (onder)uitbesteding aan DNB. Belangrijke of kritieke activiteiten hebben betrekking op de pensioenadministratie (rechtenbeheer/excasso van pensioenbetalingen) en het (fiduciair) vermogensbeheer van tenminste 30%.

Persoonsgegevens van het fonds, die door de (onder)uitbestedingspartij wordt verwerkt, worden idealiter in Nederland verwerkt en bewaard of hooguit in de Europese Unie opgeslagen maar zeker niet buiten de Europese Unie.

[1] Voor een volledige beschrijving van de governance verwijzen wij u naar paragraaf 1.2 van de Actuariële en Bedrijfstechnische Nota (ABTN)
[2] https://www.toezicht.dnb.nl/3/50-203304.jsp

De opslag van persoonsgegevens wordt beperkt tot alleen die partijen die persoonsgegevens nodig hebben voor de uitvoering van hun diensten. In alle andere situaties wordt gewerkt met geanonimiseerde bestanden/gegevens.

Met de uitbestedingspartij worden wettelijke onderzoeksmaatregelen contractueel overeengekomen (right to audit / right tot examine) ook in die situaties waarin sprake is van onderuitbesteding.

3 Strategisch kader

De uitvoering van de (primaire) diensten van Bpf Beton zijn sterk afhankelijk van IT en informatiebeveiliging. Deze afhankelijkheid maakt dat Bpf Beton kwetsbaar is voor risico's op het gebied van informatiebeveiliging en technologie. Het bestuur heeft dit onderkent en wil deze risico's adequaat beheersen.
De voortschrijdende ontwikkelingen in IT, digitalisering van processen en communicatie en de toegenomen wet- en regelgeving leiden ertoe dat informatiebeveiliging op strategisch niveau in lijn met de missie, visie en strategie wordt behandeld. Het bestuur heeft het onderstaande strategisch kader uitgewerkt.

3.1 Definitie

In dit beleid wordt onder informatiebeveiliging verstaan het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, vertrouwelijkheid en integriteit van informatie binnen Bpf Beton garanderen.

3.2 Doelstellingen

Het doel van informatiebeveiliging is om de continuïteit en betrouwbaarheid van de IT, de informatie en de informatievoorziening te waarborgen en de gevolgen van eventuele beveiligingsincidenten tot een acceptabel niveau , de door Bpf Beton vastgestelde risicobereidheid, te beperken. Cybersecurity is een integraal onderdeel van de informatiebeveiliging.

Dit betekent dat Bpf Beton de juiste maatregelen wil nemen om binnen het fonds het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van data te bereiken en te handhaven.

- Beschikbaarheid: De uitbestedingsrelatie waarborgt dat de geautoriseerde gebruikers op de juiste momenten tijdig toegang verkrijgen tot de informatie van Bpf Beton door middel van relevante bedrijfsmiddelen.
- Integriteit: De informatie van het Bpf Beton dient juist en volledig te zijn.
- Vertrouwelijkheid: Informatie is alleen toegankelijk voor de bevoegde personen.

Concreet richt het ICT-beleid zich op vijf beheersdoelen[3]:

1. deelnemerdata: behalve juistheid van deelnemersgegevens speelt bijvoorbeeld dat data niet 'op straat' komen te liggen (usb-stick) en dat communicatie zorgvuldig dient te verlopen;
2. pensioendata: aanspraken/rechten deelnemers mogen niet onterecht gewijzigd worden of verloren gaan door aanpassing van systemen of conversie van data;
3. beleggingsportefeuille: waarden mogen niet verloren gaan door bijvoorbeeld onderbreking van de beschikbaarheid van systemen of verlies van data. Juistheid van de transacties moet te allen tijde herleidbaar zijn;
4. geld/middelen op bankrekening: bescherming van waarden. Omvat bijvoorbeeld de betaling voor legitieme verleende diensten en de legitieme uitkering van pensioengelden;
5. besluitvorming en monitoring door bestuur: verkeerde of niet tijdige besluitvorming door gebreken (tijdigheid, juistheid, volledigheid) in door ICT gegenereerde informatie.

[3] Bron: Servicedocument ICT Pensioenfederatie 2015

3.3 Uitgangspunten

Awareness & In control

Het bestuur van Bpf Beton geeft richting aan het informatiebeveiliging en IT, is in staat om de uitvoering hiervan te monitoren en is in staat hierover verantwoording af te leggen aan stakeholders en de toezichthouders.

Robuustheid & wendbaarheid:

- Het streven is om IT-inrichting zo eenvoudig mogelijk te houden met als doel de kwaliteit hoog en de kosten laag te houden. Het bestuur realiseert zich daarbij dat ze daar zelf een belangrijke rol in kan spelen door bijvoorbeeld de regelingen zo eenvoudig mogelijk te houden.
- Het bestuur kiest ervoor om communicatie en uitvoering richting deelnemers te digitaliseren. Het fonds streeft met digitalisering naar een verbetering van de kwaliteit en snelheid als ook een reductie van kosten, waarbij het de intentie is dat het fonds de marktstandaarden volgt. Daarnaast moet IT ook een bijdrage aan de vernieuwing en verbetering van de dienstverlening aan deelnemers leveren.
- IT maakt het mogelijk om innovaties in de pensioenmarkt snel te adopteren. Het moet bijvoorbeeld mogelijk zijn om vereiste wijzigingen in wet- of regelgeving zeer snel en tegen lage kosten door te voeren.
- Het bestuur kiest ervoor om alle processen volgens het principe van straight through processing (STP) in te richten. Dit betekent dat de processen zonder tussenkomst van menselijk handelen worden uitgevoerd. Alleen voor processen waarbij dat onmogelijk of onwenselijk is, wordt dit in beginsel niet gedaan. Dit houdt concreet in dat er in de IT-systemen bij voorkeur een (directe) koppeling dient te bestaan met authentieke bronnen, zoals de Basis Registratie Persoonsgegevens.
- End User Computing (EUC)
  Aansluitend op het principe van STP wordt het gebruik van EUC tot een minimum teruggebracht en alleen toegepast als het niet anders kan. Indien EUC toch wordt toegepast, worden adequate beheersingsmaatregelen ingericht om te borgen dat de doelstellingen van het informatiebeveiligingsbeleid toch gerealiseerd worden.
- Bij IT-investeringsbeslissingen wordt de balans gezocht tussen niveau van gewenste dienstverlening en de daarbij behorende kosten

Betrouwbaarheid

- Het bestuur wenst dat informatieverstrekking aan deelnemers en werkgevers; de verwerking van hun gegevens; en de informatieverstrekking aan het bestuur door uitvoerders juist, tijdig en volledig gebeurt.

Beveiliging & continuïteit

Het bestuur verwacht van uitbestedingspartijen dat zij beleid en processen hebben ingericht inzake:

- Het hosten van data in de Europese Unie in geval van cloud-toepassingen met betrekking tot pensioenuitvoering.
- Het goed waarborgen van cybersecurity.
- Het goed waarborgen van business continuity.
- Inzicht in mogelijke key person risks.
- Het doelmatig en rechtvaardig gebruik van persoonsgegevens.

3.4 Risicohouding en risicobereidheidsprincipes

Het bestuur heeft de onderstaande risicohouding vastgesteld voor (niet-)financiële fondsonderwerpen zoals getoond in onderstaande tabel.

Onderdeel	Risicohouding
Financiële fondsonderwerpen (balansmanagement)	3
Niet-financiële onderwerpen (pensioenuitvoering, communicatie, IT en informatiebeveiliging, reputatie, integriteit, compliance, governance)	2
BPF Beton in het geheel	3

De risicohouding voor niet-financiële onderwerpen, zoals IT en informatiebeveiliging is Kritisch (2) : Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief laag te houden, vanuit de visie dat gewenste rewards vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd. Idealiter loopt Bpf Beton in het geheel geen risico op niet-financiële risico's maar dit is in de praktijk niet haalbaar en weegt ook niet op tegen de gevraagde extra (kosten)inspanningen.

De risicohouding is afgeleid van onderstaande tabel.

Norm	Beschrijving
Nul (1)	Deze risicohouding is gekenmerkt door de wens dat er geen risico's worden genomen, vanuit de visie dat gewenste *rewards* niet vereisen dat een minimaal niveau van blootstelling aan risico's wordt geaccepteerd.
Kritisch (2)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief laag te houden, vanuit de visie dat gewenste *rewards* vereisen dat een relatief laag niveau van blootstelling aan risico's wordt geaccepteerd.
Gebalanceerd (3)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's te balanceren, vanuit de visie dat gewenste *rewards* vereisen dat een gebalanceerd niveau van blootstelling aan risico's wordt geaccepteerd.
Opportuun (4)	Deze risicohouding is gekenmerkt door de wens de mate van blootstelling aan risico's relatief hoog te houden, vanuit de visie dat gewenste *rewards* vereisen dat een relatief hoog niveau van blootstelling aan risico's wordt geaccepteerd.
Gemaximeerd (5)	De risicohouding is gekenmerkt door de wens dat de blootstelling aan risico's maximaal is, vanuit de visie dat de gewenste *rewards* vereisen dat een maximale blootstelling aan risico's wordt geaccepteerd.

Voor de beoordeling van beleidsvoorstellen en -uitvoering heeft het bestuur voor informatiebeveiliging de risicobereidsheidsprincipes gedefinieerd. Per risicobereidheidsprincipe is aangegeven op welke wijze kan worden aangetoond dat aan het risicobereidheidsprincipe wordt voldaan (risk appetite indicator) en is de risicotolerantie aangegeven door middel van een streefwaarde inclusief een grens ondermaats en bovenmaats.
Het fonds heeft onderscheid gemaakt naar risicobereidheidsprincipes op strategisch resp. op operationeel niveau.

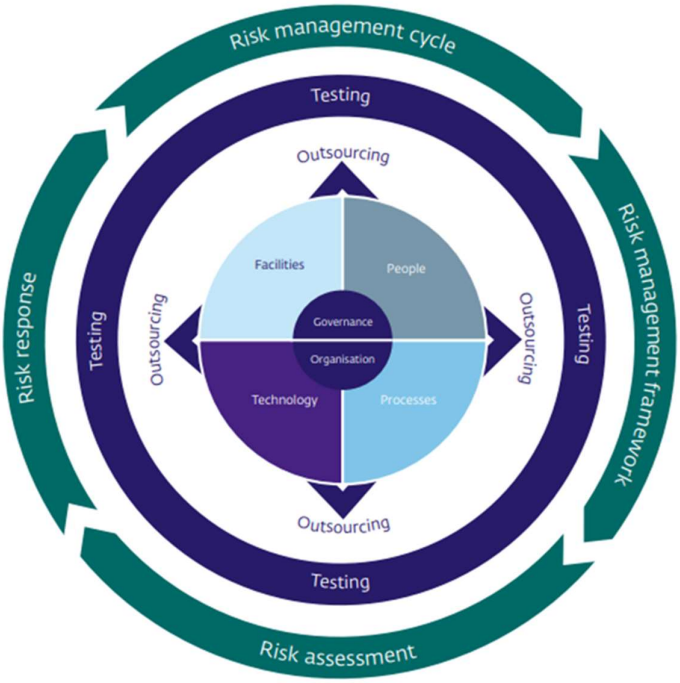
Strategisch niveau					
Nr.	**Risicobereidheidsprincipe**	**Risk appetite indicator**	**Streef-waarde**	**Onder-maats**	**Boven-maats**
1	Bestuur maakt gebruik van bewezen technologie, volgt de marktontwikkelingen en heeft niet de ambitie om daarin direct voor op te willen lopen	Jaarlijkse beoordeling en evaluatie	1	0	2
2	Wij willen dat pensioenuitvoerder innovatief is en een duidelijke roadmap heeft als het gaat om automatisering bij met een passend budget	Bespreken en evalueren met uitvoerder	1	0	2
3	IT moet zo ingericht dat noodzakelijke en/of gewenste aanpassingen met een korte doorlooptijd en tegen aanvaardbare kosten te realiseren zijn (wendbaarheid IT)	Jaarlijkse beoordeling en evaluatie	1	0	2
4	Het bestuur verlangt van de uitvoerder dat de informatiebeveiliging en borging data is ingericht en	Jaarlijkse beoordeling en evaluatie	1	0	2

	wordt uitgevoerd conform de laatste van wet- en regelgeving en technische mogelijkheden

Operationeel niveau					
Nr.	**Operationele risicobereidheidsprincipe**	**Risk appetite indicator**	**Streef-waarde**	**Onder-maats**	**Boven-maats**
1	Gegevensverwerking moet tijdig en volledig zijn, evenals communicatie naar de klant.	aantal werkdagen vertraging	0	5	0
2	Wij willen besluiten nemen op basis van meest actuele, betrouwbare, volledige data, tijdig aangeleverd door uitbestedingsrelaties/adviseurs.	aantal werkdagen vertraging	0	5	0
3	Wij willen business continuity waarborgen zodat onze uitkeringen en premieheffingen tijdig en juist zijn	Recovery time (uren)	24	36	0
4	Wij willen zicht hebben op key person risks (in onderuitbesteding) bij onze uitbestedingsrelaties	Risicoanalyse uitvoeren (per aantal jaren)	1	2	0,5

4 Uitwerking van beleid

Het bestuur heeft het beleid uitgewerkt aan de hand van de acht onderdelen van het DNB Toetsingskader Informatiebeveiliging 2019 -2020 zoals weergegeven in onderstaande figuur. De 'Risk Management Cycle' is het proces dat ervoor zorgt dat de opzet, bestaan en werking van de acht onderdelen worden gemonitord door het bestuur. De acht onderdelen zijn ieder verder opgedeeld naar in totaal 58 controls. Het totaaloverzicht van de onderdelen en de controls per onderdeel is opgenomen in bijlage 2.



4.1 Governance

4.1.1 Wet en regelgeving, standaarden en best practices

Bpf Beton verlangt van haar uitbestedingsrelaties dat zij voor de aanpak en implementatie van maatregelen op het gebied van informatiebeveiliging zich houden aan relevante wet- en regelgeving. Dit betreft onder andere:

- Pensioenwet
  - artikel 143, eerste lid; waarborgen beheerste en integere bedrijfsvoering
- Algemene Verordening Gegevensbescherming (AVG);
- Archiefwet;
- Wet verplichte deelneming in een bedrijfstakpensioenfonds 2000 (Wbpf);
- Sanctiewet (1997)
- Code Pensioenfondsen.

- Guidance uitbesteding door pensioenfondsen, uitgave van de Nederlandsche Bank N.V. van juni 2014.

Daarnaast dient rekening te worden gehouden met geaccepteerde standaarden en best practices.

4.1.2 BIV-analyse

Voor de identificatie van belangrijkste risico's geldt een rating vanuit de BIV-analyse. Dit is een analyse van de risico's van de belangrijkste systemen van de uitbestedingspartners op de onderdelen Beschikbaarheid, Integriteit en Vertrouwelijkheid. Qua indeling duiden we per categorie met 1, 2, en 3 de zwaarte van het risico aan. Waar '1' staat voor laag en '3' voor hoog risico. Met de uitbestedingspartijen wordt overeengekomen dat zij beheersmaatregelen hebben geïmplementeerd overeenkomstig het beleid van het fonds. Tevens wordt met de uitbestedingspartner per systeem een maximale uitval afgesproken. Hoe hoger het risiconiveau, hoe korter de maximale uitvaltijd. De BIV-classificatie is opgenomen in bijlage 1 van dit document.

Beschikbaarheid

De uitbestedingsrelatie waarborgt dat de geautoriseerde gebruikers op de juiste momenten tijdig toegang verkrijgen tot de informatie van Bpf Beton door middel van relevante bedrijfsmiddelen. De uitvoeringssystemen zijn beveiligd en bij uitval geldt een maximale recovery tijd. Daarover spreekt het Bpf Beton met de uitbestedingsrelatie de grenzen van recovery af.

Integriteit

De informatie van het Bpf Beton dient juist en volledig te zijn. Daartoe zet de uitbestedingsrelatie de relevante bedrijfsmiddelen in en overlegt deze met het bestuur van het pensioenfonds.

Vertrouwelijkheid

Informatie is alleen toegankelijk voor de bevoegde personen. Bestuurders, leden van de Raad van Toezicht en het Verantwoordingsorgaan gaan vertrouwelijk om met informatie. Daarbij maakt het pensioenfonds gebruik van een beveiligd digitaal platform voor alle fondsdocumenten en vergaderstukken. In voorleggers wordt op anonieme wijze gesproken over belanghebbenden van het pensioenfonds.

Met de uitbestedingsrelatie komt Bpf Beton overeen wie als bevoegde personen kunnen worden aangewezen. Functiescheiding wordt toegepast om het botsen van belangen tegen te gaan en de kans op frauduleus handelen te beperken.

Het management van de uitbestedingsrelatie is verantwoordelijk voor het opstellen, inrichten en naleven van het beleid.

4.2 Organisatie

Het bestuur is eindverantwoordelijk voor een adequate organisatie van taken, verantwoordelijkheden en bevoegdheden en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst zoals onder meer:

- het bestuur heeft taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cybersecurity helder belegd.
- het bestuur beschikt, gegeven de risicohouding, over voldoende capaciteit, kennis en ervaring om invulling te geven aan deze taken en verantwoordelijkheden.

- het bestuur draagt actief en zichtbaar het belang uit van informatiebeveiliging en cybersecurity voor Bpf Beton en haar uitbestedingspartijen.
- Goed opdrachtgeverschap: het bestuur ziet erop toe dat de aangestelde uitbestedingspartijen gemaakte afspraken nakomen over het beleggen van taken en verantwoordelijkheden voor informatiebeveiliging en cybersecurity, eigenaarschap van gegevens en informatiesystemen en functiescheiding in hun organisaties.

4.2.1 Assurance

Het Bpf Beton heeft voor het integrale risicomanagement een IRM commissie ingesteld. Deze commissie evalueert jaarlijks de informatiebeveiligingsmaatregelen en beoordeelt of de gestelde doelen zijn bereikt. Daarover rapporteert de IRM commissie aan het bestuur van het pensioenfonds. De uitbestedingsrelatie legt jaarlijks verantwoording af over het geheel van interne beheersmaatregelen door een verklaring van zijn externe accountant middels een ISAE 3402/3000 verklaring, vergelijkbare verklaring en/of Third Party Memorandum (TPM) en rapportages niet-financiële risico's. Op verzoek van het fonds worden gesprekken aangevraagd waarin specifieke thema's inhoudelijk nader worden behandeld.

4.2.2 Audit

Het Bpf Beton stelt als voorwaarde dat de uitbestedingsrelatie periodiek audits uitvoeren op de opzet, werking, bestaan van de beheersmaatregelen van informatiebeveiliging in relatie tot de risico's.
Bevindingen van deze audits worden met het bestuur van Bpf Beton besproken. Ook op initiatief van Bpf Beton en/of de sleutelfunctiehouder interne audit kunnen audits worden uitgevoerd.

4.3 Mensen (People)

Het is belangrijk dat alle medewerkers, externe inhuur en dienstverleners bekend zijn met het informatiebeveiligingsbeleid van Bpf Beton, hun verantwoordelijkheden kennen en kunnen (blijven) werken volgens dit beleid en de risicobereidheid van Bpf Beton. Het bestuur is eindverantwoordelijk voor het (blijvend) zorgdragen voor een passend kennisniveau van medewerkers en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst.
Goed opdrachtgeverschap: het bestuur ziet erop toe dat de uitbestedingspartijen hun afspraken nakomen ten aanzien van de personele aspecten van informatiebeveiliging en cybersecurity zoals hierboven genoemd.

4.3.1 Bestuur en personeel

Bestuurders, leden van organen van het pensioenfonds en personeel van de uitbestedingsrelaties worden voorafgaand aan het dienstverband geïnformeerd over de verantwoordelijkheden ten aanzien van informatiebeveiliging. Deze verantwoordelijkheden zijn voor bestuurders (verbonden personen) vastgelegd in de gedragscode van het pensioenfonds. De gedragscode is op de site van Bpf Beton beschikbaar. Voor personeel van de uitbestedingsrelatie geldt dat zij middels de (arbeids)overeenkomst en functiebeschrijvingen worden geïnformeerd.
Voorafgaand aan het lidmaatschap binnen het bestuur vindt een screening plaats. Dat geschiedt via de gemeente door een Verklaring Omtrent het Gedrag op te vragen. Nadere omschrijving van de screening is beschikbaar in het screeningsbeleid.
De uitbestedingsrelatie zorgt ervoor dat voorafgaand aan een dienstverband van haar medewerker(s) altijd een Pre Employment Screening (PES) van de medewerker plaatsvindt. Verder

moeten medewerkers mee werken aan een verzoek tot screening en/of het verstrekken van een Verklaring Omtrent het Gedrag (VOG).
Tijdens en na beëindiging van het bestuurslidmaatschap dan wel de (arbeids)overeenkomst van de werknemers van uitbestedingsrelaties, zijn bestuurders, medewerkers, ingehuurd personeel en externe gebruikers verplicht tot geheimhouding van alle informatie en/of kennis die hij/zij heeft gekregen over Bpf Beton, de eigen organisatie, gelieerde ondernemingen en opdrachtgevers van de organisatie.

4.3.2 Bewustzijn, opleiding en training
Bestuurders en andere verbonden personen verklaren door het ondertekenen van de gedragscode dat zij zich bewust zijn van het infomatiebeveiligingsbeleid en de afspraken ten aanzien van vertrouwelijkheid en geheimhouding.
Medewerkers van uitbestedingsrelaties volgen een passende bewustwordingstraining welke de uitbestedingsrelatie faciliteert. (BMO traint jaarlijks haar medewerkers op dit vlak).

4.3.3 Sancties
Indien het bestuur constateert dat een verbonden persoon zich niet houdt aan de gestelde richtlijnen van informatiebeveiliging, gaat het in gesprek met betreffende persoon. Alleen als blijkt dat het om een bewust ongeoorloofd handelen gaat zal het bestuur passende maatregelen treffen. *(sancties met betrekking tot ongeoorloofd handelen bij de uitbestedingsrelatie dienen aldaar te zijn vastgelegd en uitgevoerd)*

4.3.4 Beëindiging bestuurderschap of het dienstverband
Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging van het bestuurder lidmaatschap zijn verankerd in de gedragscode. De uitbestedingsrelatie communiceert aan zijn werknemer(s) bij beëindiging van het dienstverband welke verantwoordelijkheden ook na het eindigen van de arbeidsovereenkomst van kracht blijven. Tevens worden toegangsrechten en user-id's verwijderd, en bedrijfsmiddelen ingeleverd.

4.4 Processen
Het bestuur is eindverantwoordelijk voor het zorgdragen en/of controleren dat de strategie en het overall IT-security plan in lijn is met de richtlijnen van het bestuur en de overige bedrijfsprocedures met betrekking tot:

- Continuïteit van de operatie.
- Het beheersen van incidenten inclusief beleid inzake escalatie.
- Het op beheerste wijze wijzigingen doorvoeren zonder verstoring van het informatiebeveiligingsniveau en/of de data-integriteit negatief beïnvloeden.
- Het uitvoeren van de testprocedures afgescheiden van de productieomgeving.
- De kwaliteit van de IT-beheerprocessen.

4.4.1 Melden van (beveiligings)incidenten
Informatiebeveiligingsincidenten en eventuele geconstateerde zwakke plekken in de beveiliging, worden door het bestuur van het pensioenfonds direct besproken en verholpen. Wijzigingen in het informatiebeveiligingsbeleid worden met de verbonden personen en uitbestedingsrelaties binnen twee weken na vaststelling gecommuniceerd. Zwaarwegende incidenten worden aan DNB gemeld.

Incidenten dan wel constatering van zwakke plekken bij de uitbestedingsrelatie en haar (eventuele (toe)leveranciers behoren onverwijld te worden gerapporteerd aan Bpf Beton en toegelicht. Van de incidenten op het vlak van informatiebeveiliging wordt een incidentenregister bijgehouden.

4.4.2 Bedrijfsmiddelen
Voor de werknemer van een uitbestedingsrelatie geldt dat (bedrijfs)middelen die toegang en/of autorisatie faciliteren tot informatie en deze kunnen opslaan, ondersteunen en/of essentieel zijn binnen de bedrijfsvoering, worden geregistreerd en gekoppeld aan een eigenaar. De uitbestedingsrelatie is verantwoordelijk voor de juiste classificatie en de toegepaste beveiligingsmaatregelen.

4.4.3 Opslag van informatie
Het Bpf Beton slaat informatie zoveel mogelijk digitaal op. Opslag vindt plaats via OurMeeting, een beveiligde omgeving waar een strikte autorisatiescheiding is toegepast. Verbonden personen krijgen alleen toegang tot de voor hen relevante informatie. In het privacyreglement staat beschreven op welke wijze het pensioenfonds omgaat met (persoons)gegevens en hoe lang deze worden bewaard. De fondsspecifieke informatie wordt door de dienst “bestuursondersteuning” op een alleen voor hen toegankelijke schijf opgeslagen. De pensioenuitvoeringsorganisatie faciliteert en bewaakt dit proces. De uitbestedingsrelatie draagt er zorg voor dat informatie(dragers) worden bewaard op een locatie met beveiligingsmaatregelen die in overeenstemming zijn met de classificatie van de betreffende informatie.

4.4.4 Printen van informatie

Bij het printen van informatie zijn de verbonden personen gehouden zorgvuldig om te gaan met de output. Indien het fysieke stuk niet langer hoeft te worden bewaard, wordt de print vernietigt. Vanwege de gevoelige klantinformatie die beschikbaar is bij de uitbestedingsrelatie(s), past de uitbestedingsrelatie een beveiligd printsysteem toe.

4.4.5 Verstrekken van informatie
De uitbestedingsrelatie verstrekt (deelnemer) informatie bij voorkeur via de standaard digitale of schriftelijke kanalen.
Het telefonisch verstrekken van deze informatie is pas toegestaan wanneer vaststaat dat het de deelnemer of een gemachtigde derde betreft. Dan wel een aan de uitbestedingsrelatie verbonden persoon. Er bestaat een protocol waarmee de identiteit van de informatievrager wordt vastgesteld.

4.4.5 Verstrekken van fonds informatie
Het verstrekken van fondsinformatie aan derden (bijvoorbeeld DNB, AFM), voor zover dit niet wettelijk verplicht is, vindt pas plaats na schriftelijk akkoord van het fonds.

4.4.6 Verwijderen en vernietigen van informatie
Verwijderen en vernietigen van informatie vindt gecontroleerd plaats conform de afspraken tussen het pensioenfonds en de uitbestedingsrelatie. Daarbij gelden de volgende uitgangspunten:

Onderwerp	V1 Openbaar	V2 Intern gebruik	V3 Vertrouwelijk
Verwijderen digitale media	Vrij	Delete; Bij levering media aan derden: via speciale tooling	Afvoeren en vernietigen door een gespecialiseerde organisatie onder overhandiging van certificaat. Voor het verwijderen van fonds en klantinformatie bestaat een protocol.
Verwijderen papieren documenten	Vrij	Papierbak/afgesloten container.	Afgesloten container/shredder

4.4.7 Bewaartermijnen

Fonds- en deelnemer informatie wordt bewaard zoals beschreven in het privacyreglement en zoals afgesproken in de contracten met uitbestedingsrelaties. Voor het verwijderen en vernietigen van informatie in geval van einde bewaartermijn hanteert de uitbestedingsrelatie een vaste procedure in lijn met het privacyreglement van Bpf Beton.

4.4.8 Wijzigingsbeheer

Het up-to-date houden van programmatuur is van groot belang om kwetsbaarheden te beperken. Hierdoor is het noodzakelijk dat o.a. notebooks periodiek de updates kunnen installeren. Updates worden vaak automatisch uitgevoerd.

4.4.9 Scheiding Ontwikkel-Test-Productie omgevingen

Om te zorgen dat databases van de uitbestedingsrelatie niet bevuild raken met testgegevens en/of productiegegevens onbedoeld in een testomgeving terecht komen, is het van belang dat in elke fase van software ontwikkeling goed overwogen wordt welke (test)gegevens nodig zijn en hoe deze gegevens eruit zien. Er worden geen productiegegevens van Bpf Beton gebruikt, gegevens worden (zoveel mogelijk) geanonimiseerd en het aantal aangeleverde velden zo beperkt mogelijk gehouden. Voor verzending van deze geanonimiseerde testbestanden wordt gebruik gemaakt van een wijze van versleuteling. Afspraak hierbij is dat separaat een wachtwoord wordt verstuurd via een niet publiekelijk toegankelijk kanaal (bijv. mondeling/sms).

4.4.10 Leveranciersrelaties

Uitbestedingsrelaties doen zaken met (vele) leveranciers. Het is van groot belang dat deze leveranciers voortdurend passende maatregelen nemen om de informatie te beveiligen en de continuïteit van de onderneming te waarborgen. Daar waar van toepassing hanteert de uitbestedingsrelatie ten aanzien van de specifieke informatiebeveiligingsaspecten de volgende uitgangspunten:

- Indien de uitbestedingsrelatie gebruik maakt van (toe)leveranciers dan gelden voor hen minimaal dezelfde (informatiebeveiligings)eisen als het Bpf Beton stelt voor de uitbestedingsrelatie.
- De uitbestedingsrelatie neemt alleen producten en/ of diensten van (toe)leveranciers af die voldoen aan de gestelde beveiligingseisen van Bpf Beton voor dat product of die dienst.
- De uitbestedingsrelatie documenteert de (toe)leveranciers en rapporteert daarover aan het bestuur van Bpf Beton.

Daar waar van toepassing worden in alle leverancierscontracten en bijhorende SLA afspraken de relevante afspraken en rechten en plichten van beide partijen op het gebied van informatiebeveiliging opgenomen (informatiebeveiligingsparagraaf).
Uitgangspunten binnen de betreffende informatiebeveiligingsparagraaf zijn:

- Dienstverlening van Leverancier is compliant aan geldende wet- en regelgeving;
- Leverancier conformeert zich aan het Informatiebeveiligingsbeleid van Bpf Beton;
- Het beveiligingsniveau binnen de dienstverlening door Leverancier voldoet minimaal aan het geldende (basis)niveau van beveiliging van Bpf Beton;
- Leverancier geeft zekerheden ten aanzien van het overeengekomen niveau van informatiebeveiliging (bijvoorbeeld certificaat, derden verklaring);
- De uitbestedingsrelatie heeft het recht om de informatiebeveiliging binnen de dienstverlening met (toe)leveranciers periodiek te beoordelen (audit);
- Er worden afspraken gemaakt over incidentafhandeling, communicatie en het informeren van het bestuur van Bpf Beton in geval van een incident en/of datalek bij de (toe)leverancier.

4.4.11 Datalek

Een zogenaamd 'datalek' is een bijzondere vorm van een security incident, waarbij persoonsgegevens betrokken zijn. Datalekken moeten onverwijld binnen 24 uur aan het bestuur van Bpf Beton worden gemeld en binnen 72 uur aan de Autoriteit Persoonsgegevens.
Onder datalek verstaan we ieder incident bij verwerking van persoonsgegevens door de pensioenuitvoerder, waarbij sprake is van een inbreuk in verband met persoonsgegevens zoals bedoeld in de Algemene Verordening Gegevensbescherming. Op grond van de AVG dient ieder datalek te worden gemeld, tenzij het niet waarschijnlijk is dat inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De pensioenuitvoerder informeert het bestuur bij een datalek over:

- de aard en omvang van de inbreuk op de beveiliging;
- de naam en contactgegevens van degene bij wie meer informatie over de inbreuk kan worden verkregen;
- de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van Persoonsgegevens en (kring van) de betrokkenen;
- de maatregelen die zij heeft getroffen of voorstelt te treffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen;
- aanvullende gegevens die het fonds nodig heeft om een eventuele melding bij de toezichthouder te kunnen verrichten.

Binnen 72 uur beoordeelt het bestuur de melding van een (mogelijk) datalek en bepaalt daarbij of er melding aan de Autoriteit Persoonsgegevens plaats dient te vinden.
Elke melding staat op zich en Bpf Beton zal ultimo 2021 de ervaringen van (gemelde) datalekken evalueren om op grond daarvan te bezien of eenduidige criteria kunnen worden benoemd wanneer er melding aan de AP plaats dient te vinden.

4.4.12 Continuïteit management

De continuïteit van de bedrijfsvoering van de uitbestedingsrelatie is van significant belang. De uitbestedingsrelatie neemt maatregelen om de continuïteit te waarborgen en rapporteert daarover tijdens de jaarlijkse evaluatie.

4.4.13 Business Impact Analyse

De uitbestedingsrelatie stelt de gewenste minimale mate van beschikbaarheid jaarlijks, en in ieder geval bij relevante wijzigingen, vast door middel van een Business Impact Analyse (BIA). Binnen deze BIA wordt een kwalitatieve inschaling van de verwachte impact vastgesteld van een gebeurtenis die leidt tot het niet beschikbaar zijn van de betreffende informatie(voorziening) gedurende een bepaalde tijd. Ook wordt binnen de BIA de maximaal acceptabele mate van dataverlies bepaald. De BIA dient te worden uitgevoerd in de gevallen waarbij de keuze voor / selectie van continuïteit verhogende maatregelen (bijv. dubbel uitvoeren systemen, uitwijkregeling, eisen aan leveranciers) voor ligt.

4.4.14 Business Continuity Plan

De uitbestedingsrelatie stelt een Business Continuity Plan (BCP) op, gericht op het adequaat omgaan met gebeurtenissen die de beschikbaarheid van de informatievoorziening op centraal bedrijfsniveau raakt. Binnen dit plan is een continuïteitsorganisatie gedefinieerd, waarbinnen een Crisis Management Team (CMT) een centrale positie inneemt.

De uitbestedingsrelatie stelt voor zichzelf en voor de bedrijfsprocessen en (IT-)bedrijfsmiddelen van derden in beheer, een continuïteitsplan op inclusief een uitwijkplan.

4.4.15 Uitwijkvoorziening
De uitbestedingsrelatie maakt gebruik van een beveiligde uitwijkvoorziening zoals bijvoorbeeld een "Twin Data Center". De beveiliging geschiedt conform de normen en richtlijnen voor de afzonderlijk behandelde onderdelen in dit Informatiebeveiligingsbeleid. Voor zover hierbij gebruik wordt gemaakt van de diensten van derden worden hiervoor Third Party Memorandums (TPM's) opgesteld.

4.4.16 Back-up en recovery
De uitbestedingsrelatie maakt dagelijks back-ups van gegevens en programmatuur om bij verstoringen de gegevens te kunnen herstellen. Periodiek (minimaal jaarlijks) wordt een back up and recovery test uitgevoerd.

4.5 Technologie

4*.5.1 Autorisatie*
Ten aanzien van autorisaties gelden de volgende voorwaarden:
- een gebruiker (medewerker van de uitbestedingsrelatie) wordt geïdentificeerd met een unieke user-id;
- user-id's en wachtwoorden zijn persoonsgebonden en niet overdraagbaar;
- user-id's en wachtwoorden mogen niet worden gedeeld;

Het management van de uitbestedingsrelatie is verantwoordelijk voor het toekennen van autorisaties.

4.5.2 Wachtwoorden

Wachtwoorden dienen minimaal te voldoen aan de volgende kenmerken:
- minimale lengte: 8 karakters;
- gebruik van combinatie van hoofdletters, kleine letters, leestekens, cijfers;
- vermijdt reguliere woorden en/of eenvoudig herleidbare namen;
- wachtwoorden dienen periodiek (minimaal jaarlijks) gewijzigd te worden.

4.5.3 Toegang via (mobiele) devices
Devices (apparatuur) die worden gebruikt om toegang te verkrijgen tot het netwerk van de uitbestedingsrelatie dienen zogenaamde managed devices te zijn. De uitbestedingsrelatie beheert en bewaakt deze devices.

4.5.4 Externe toegang
Het netwerk van de uitbestedingsrelatie mag alleen van buiten betreffende locatie van de relatie benaderd worden via een versleutelde verbinding en two-factor authenticatie.

4.5.5 Authenticatie
De authenticatie van gebruikers dient minimaal te voldoen aan de 'two-factor' standaard. Dit wil zeggen dat de authenticatie minimaal twee van de volgende authenticatiefactoren vereist: Iets wat je weet (bijv. wachtwoord, pincode), iets wat je hebt (bijv. token, pasje, managed device/certificaat), iets wat je 'bent' (bijv. vingerafdruk, iris-scan).

4.5.6 High privileged accounts
Het gebruik van accounts met hoge rechten (high privileged accounts), zoals root- en beheerdersaccounts is slechts toegestaan als deze noodzakelijk zijn voor de uitvoering van specifieke beheertaken. Hiervoor dienen de gebruikers van deze accounts een schriftelijk akkoord te hebben van de uitbestedingsrelatie. Na afronding van de werkzaamheden moet het account direct geblokkeerd worden. Elk gebruik van high privileged accounts moet gelogd en gemonitord worden.

4.5.7 Cryptografie
Opslag en transport van informatie door de uitbestedingsrelatie met een bepaalde mate van vertrouwelijkheid (V2 of V3), dient op een versleutelde wijze te gebeuren.

4.5.8 Opslag op digitale media
Wanneer opslag van informatie met classificatie V3 op digitale verwijderbare media plaatsvindt (bijv. externe schijf, usb-device), dient de informatie versleuteld te zijn.

4.5.9 Bestanden
Daar waar dat door wet- en regelgeving wordt gevraagd en/of wanneer dit bijvoorbeeld vanwege de specifieke aard van de informatie wenselijk wordt geacht, worden bestanden die informatie met classificatie V3 bevatten, voorzien van een (sterk)wachtwoord. Het wachtwoord moet op een veilige, separate locatie (dus niet op dezelfde schijf) opgeslagen worden en via een separaat kanaal gecommuniceerd worden.

4.5.10 Databases

Daar waar dat door wet- en regelgeving wordt gevraagd en/of wanneer dit bijvoorbeeld vanwege de specifieke aard van de informatie wenselijk wordt geacht (bijv. in geval van persoonsgegevens), worden databases die informatie met classificatie V3 bevatten, adequaat versleuteld. De sleutel dient separaat en adequaat beheerd te worden.

4.5.11 E-mail
Voor e-mail past het bestuur van Bpf Beton een beveiligde omgeving toe. Alle e-mailadressen van de bestuursleden zullen worden gefaciliteerd via een speciaal beveiligde omgeving vanuit de pensioenuitvoeringsorganisatie. De uitvoeringsorganisatie werkt aan de inrichting van het beoogde mailverkeer.
Informatie met classificatie V3 wordt niet via e-mail verspreid. In die gevallen wanneer verzending noodzakelijk is, wordt gebruik gemaakt van File Transfer of een andere wijze van versleuteling. Afspraak hierbij is dat separaat een wachtwoord wordt verstuurd via een niet publiekelijk toegankelijk kanaal (bijv. mondeling/sms).

4.5.12 Beheersmaatregelen tegen malware
De uitbestedingsrelatie neemt technische maatregelen om malware en virussen ‘buiten de deur’ te houden. De medewerker van de uitbestedingsrelatie wordt geacht er voor te zorgen dat besmetting door/met malware zo veel als mogelijk wordt voorkomen.

4.5.13 Communicatiebeveiliging
Het netwerk van de uitbestedingsrelatie dient met (diverse) technische en organisatorische maatregelen te zijn beveiligd en worden beheerd. Het uitgangspunt hierbij is dat er een zogenaamde gelaagde beveiliging plaatsvindt. Het idee achter deze benadering is dat systemen en informatie wordt beschermd tegen aantasting van de Vertrouwelijkheid, Integriteit en Beschikbaarheid, met behulp van verschillende onafhankelijke methoden en technieken. De betreffende maatregelen variëren in aard.
Zo is er onderscheid te maken in: preventieve, detectieve, correctieve en repressieve maatregelen. Wanneer er binnen de werkzaamheden gebruik kan worden gemaakt van een thuisnetwerk-omgeving, dient deze omgeving adequaat beveiligd te zijn. Dat wil zeggen dat deze omgeving minimaal is voorzien van de laatste beveiligingsupdates, firewall-functionaliteit, bescherming tegen malware. Ook is het wenselijk om het standaardwachtwoord van een Wifi-access point te wijzigen.

4.5.14 Het beheer van de netwerkbeveiliging
Het beheer van de netwerkbeveiliging vindt gestructureerd plaats op basis van de principes van procesmatig IT service management . De uitbestedingsrelatie informeert het bestuur op welke wijze het beheer plaatsvindt.

4.5.15 Scheiding in netwerken
Vanuit beveiligingsperspectief is het van belang dat netwerken met een onderling afwijkende gebruiksaard en/of gebruikersdoelgroep (gasten / klanten / beheer / demo / test / productie) logisch dan wel fysiek van elkaar zijn gescheiden.

4.6 Faciliteiten

4.6.1 Clouddiensten
Er gelden restricties ten aanzien van het gebruik van clouddiensten. Het toegestane gebruik van dergelijke diensten gekoppeld aan de classificatie van de informatie. De diensten worden door de uitbestedingsrelatie gehost en beheerd vanuit een datacenter van een service provider die door de uitbestedingsrelatie is aangesteld.

4.6.2 Fysieke beveiliging en beveiliging van de omgeving
Fysieke beveiliging omvat het fysiek afschermen, beschermen en afsluiten van ruimten met geschikte beveiligingsbarrières en toegangsbeveiliging om aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te voorkomen.

4.6.3 Algemene toegang
Ten aanzien van de algemene toegang van bedrijfsruimte en afdelingen wordt als uitgangspunt gehanteerd dat de uitbestedingsrelatie toeziet op autorisatie. Bezoekers melden zich bij de receptie en worden gedurende het bezoek begeleid. Ook krijgen zij een bezoekerspas.

4.7 Uitbesteding
Het fonds heeft het pensioenbeheer en de het vermogensbeheer uitbesteed aan externe partijen omdat het fonds meent dat externe partijen de werkzaamheden van kwalitatief hoog niveau op efficiënte wijze kunnen uitvoeren in vergelijking tot eigen beheer door fonds zelf.

Uitbesteding brengt naast voordelen ook risico's met zich mee op het gebied van informatiebeveiliging en cybersecurity. Onderdeel van het selectieproces is het opstellen van een risico-analyse. Tijdens het uitbestedingsproces wordt afspraken gemaakt over:

- De naleving van het informatiebeveiligingsbeleid van het fonds door de uitbestedingspartij. Uitgangspunt is dat voldaan wordt aan de 58 beheersingsmaatregelen in het normenkader informatiebeveiliging van DNB 2019-2020.
- De wijze waarop de uitbestedingspartij rapporteert over o.a. informatiebeveiliging en beheersing van het cybersecurity risico inclusief eventueel aangestelde subcontractors.
- De uitbestedingspartner stuurt bij op het moment dat risicotoleranties worden overschreden.

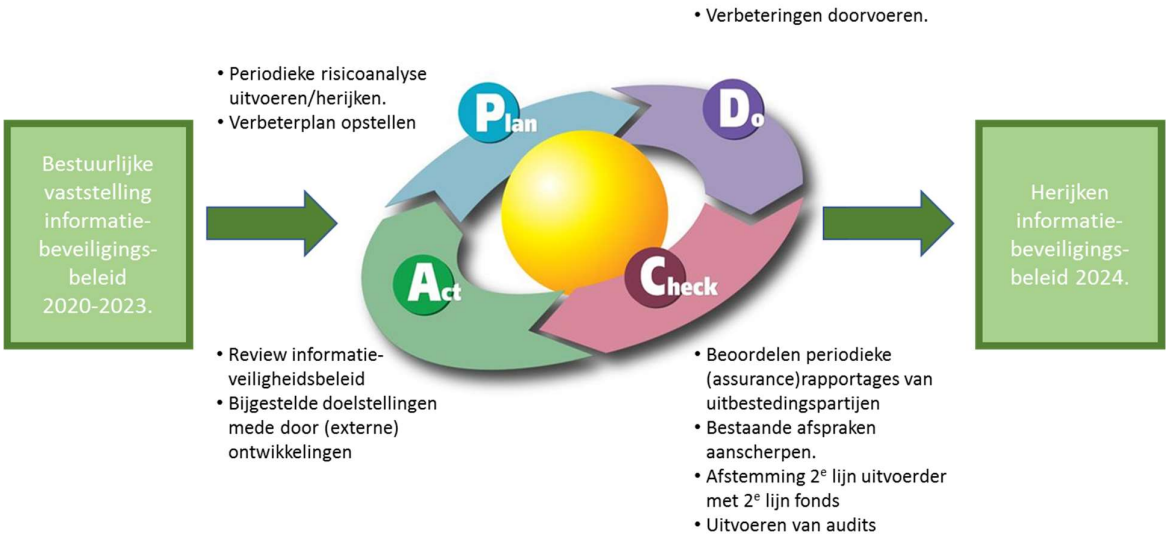
Het uitbestedingsbeleid van het fonds is leidend voor de uitvoering van het selectieproces. Het selectieproces wordt uitgevoerd in lijn met de DNB Guidance uitbesteding door pensioenfondsen (juni 2014).

4.8 (Security) Testing

Het bestuur ziet erop toe dat er periodiek security testing plaats vindt op de diverse onderdelen van het model bijvoorbeeld technologie, mensen, faciliteiten. Het fonds kan dat zelf uitvoeren of een derde daartoe opdracht geven. Ook kan het uitgevoerde beheersmaatregelen zoals deze door de uitbestedingspartij onafhankelijk laten testen door een daartoe aangestelde externe partij. Security testing is bedoeld het bestuur een onafhankelijk volledig en transparant beeld te verstrekken over de geteste onderdelen met het doel te kunnen beoordelen of de processen voldoende robuust zijn of aanpassing vergen.

4.9 (Risicomanagement) Proces

In de uitvoering van dit beleidsdocument informatieveiligheid maakt het bestuur gebruik van de Plan-Do-Check-Act cyclus zoals onderstaand weergegeven.



Plan

Het bestuur is verantwoordelijk voor de uitvoering van dit beleid. De uitvoering van het informatiebeveiligingsbeleid is gedelegeerd aan de IRM-commissie. De IRM-commissie voert regie op de uitvoering van het beleid en stelt hiertoe een jaarkalender op.

De uitkomsten uit de periodieke risicoanalyse kunnen aanleiding geven tot het opstellen van een verbeterplan. Met de uitbestedingspartijen zijn/worden afspraken gemaakt over naleving van het informatiebeveiligingsbeleid. Daarbij streeft Bpf Beton ernaar te komen tot een sluitende rapportagelijn tussen het fonds en de uitbestedingspartij. De eisen van het fonds worden in overleg met de uitbestedingspartijen vastgesteld en sluiten aan op het DNB self assessment informatieveiligheid. De belangrijkste eisen zullen vervolgens ook in de SLA met de betreffende uitbestedingspartijen worden opgenomen, inclusief afspraken over de wijze van rapportage. Indien een leverancier niet kan voldoen aan deze eisen, wordt hij uitgesloten.

Bpf Beton sluit zich aan bij (internationaal) erkende standaarden op IT-gebied, zoals de 58 controls van het DNB self assessment informatieveiligheid vanaf 2019, ITIL en SANS20. Bij uitbesteding toetst Bpf Beton, als één van de (potentiële) klanten, of de uitbestedingspartner voldoet aan het IT-beleid van het fonds, de wet- en regelgeving en het DNB IT Toetsingskader. Bij het afsluiten van het contract met de beoogde uitbestedingspartij moet echter duidelijk zijn dat de risico's van Bpf Beton worden beheerst. Tegelijkertijd wordt het contract met de uitbestedingspartij beoordeeld op een sluitende rapportagelijn met betrekking tot informatiebeveiliging.

Het fonds moet voldoen aan de controls zoals gedefinieerd in het DNB IT Toetsingskader. Periodiek vraagt het fonds de door de aangestelde uitbestedingspartijen ingevulde DNB IT Toetsingskader op en beoordeelt deze en indien nodig stemt deze nader af met de uitbestedingspartij. Daarnaast wil Bpf Beton de specifieke risico's voor de pensioensector in Nederland afdekken, in aanmerking nemend dat Bpf Beton geen risico's heeft die nóg specifieker zijn. Bpf Beton beschouwt de beheersing van de privacy en het cybersecurity risico als de voornaamste risico's. De kans dat deze risico's zich voordoen zijn het grootst bij de pensioenadministrateur.

Do

De IRM-commissie zorgt voor de uitvoering en waar nodig implementatie van het verbeterplan. De uitkomsten worden gerapporteerd aan het bestuur. Indien besluitvorming van het bestuur nodig is dan legt de IRM-commissie een advies voor aan het bestuur ter bekrachtiging.

Check

De uitbestedingspartners managen de beheersingsmaatregelen in de uitvoeringsfase (Deliver and Support). Het bestuur laat zich hierover informeren via SLA-rapportages, ISAE 3402 rapporten en eventuele andere (niet-financiële) rapportages of relevante certificaten zoals ISO 27001 of 27002.

Naast deze standaardrapportages laat het bestuur zich informeren over

- incidenten en de afhandeling daarvan;
- datalekken en de afhandeling daarvan;
- belangrijke stappen in strategische projecten, afhankelijk van de afspraken terzake.

De belangrijkste activiteiten bestaan uit het beoordelen van de SLA-rapportages, de ISAE-3402-type 2 rapporten en aanvullende rapportages over incidenten en datalekken. De IRM-commissie voorziet het bestuur van haar bevindingen en aanbevelingen bij deze rapportages.

Act

Het beleid wordt voor drie jaar vastgesteld. Evaluatie van het beleid gebeurt eens in de drie jaar of eerder als daartoe aanleiding bestaat. Het herijken van de risicoanalyse kan eveneens nieuwe input leveren om het informatiebeveiligingsbeleid aan te passen.

5 Inbedding in integraal risicomanagement

Het informatiebeveiligingsbeleid maakt onderdeel uit van het integraal risicomanagementbeleid van het pensioenfonds. Hiermee is zeker gesteld dat het informatiebeveiligingsbeleid de beleidscyclus doorloopt waarmee ook monitoring en evaluatie terugkeren op de bestuursagenda.

6 Verantwoording

Over de beheersing van informatiebeveiliging legt het pensioenbestuur verantwoording af aan de Raad van Toezicht en informeert het verantwoordingsorgaan.

7 Bekendmaking beleid

Het informatiebeveiligingsbeleid wordt periodiek onder de aandacht gebracht van het bestuur en de verbonden personen en uitbestedingsrelaties. Het bestuur draagt er zorg voor dat iedere nieuwe verbonden persoon bij infunctietreding de beschikking heeft over het informatiebeveiligingsbeleid van het pensioenfonds. Een wijziging van dit beleid communiceert Bpf Beton schriftelijk aan hen op wie het beleid van toepassing is. Daarnaast publiceert het fonds het informatiebeveiligingsbeleid op de website.

8 Inwerkingtreding beleid

Het informatiebeveiligingsbeleid is voor het laatst vastgesteld in de bestuursvergadering van 17 december 2021. Het informatiebeveiligingsbeleid is gewijzigd door als bijlage het EUC-beleid toe te voegen. Het IT-beleid versie 4.0 dat was vastgesteld op 26 januari 2018 was in 2020 al komen te vervallen door het te integreren in dit beleidsdocument.

Bijlage 1: BIV-classificatie

Beschikbaarheid			
classificatie	niveau	typering	Omschrijving
1	Laag	Relevant	Informatie dient over het algemeen beschikbar te zijn. Niet beschikbaarheid is beperkt acceptabel.
2	Gemiddeld	Noodzaak	Informatie dient bijna altijd beschikbaar te zijn.
3	Hoog	prioriteit	Uitval van informatie alleen in geval van calamiteiten.

Integriteit			
classificatie	niveau	typering	Omschrijving
1	Laag	Geborgen	Basis voor een juist bedrijfsproces met betrekking tot Integriteit. Fouten zijn beperkt toelaatbaar.
2	Gemiddeld	Prominent	Het bedrijfsproces is bijna foutloos.
3	Hoog	Onvoorwaar-delijk	Het bedrijfsproces is foutloos.

Vertrouwelijkheid			
classificatie	niveau	typering	Omschrijving
1	Laag	Confidentieel	Informatie is toegankelijk voor geselecteerde groep van: verbonden personen en medewerkers van een uitbestedingsrelatie. Autorisatierechten worden functiegericht toegekend.
2	Gemiddeld	Vertrouwelijk	Informatie is alleen toegankelijk voor specifiek geselecteerde groep van: verbonden personen en medewerkers van een uitbestedingsrelatie. Autorisatierechten worden functiegericht toegekend.
3	Hoog	Geheim	Informatie is geheim, alleen een beperkt aantal verbonden personen en medewerkers van een uitbestedingsrelatie verkrijgen toegang. Autorisatierechten wordt individueel toegekend.

De classificaties op hoofdcategorieën gelden voor de onderliggende subcategorieën, tenzij anders is ingevuld				
Type	**B**	**I**	**V**	**Omschrijving**
Bestuursgegevens	1	2	2	Met name beschikbaar voor bestuursondersteuning en relatiebeheer
NAW				
Identiteit				
06				
Communicatie DNB/AFM				
Communicatie				
Fondsgegevens	2	1	2	Beschikbaar voor Bestuur en adviesdiensten
Uitbestedingscontracten				
DVO/SLA				
Vacatievergoedingen				Alleen op totaalniveau inzichtelijk t.b.v. belastingaangifte
Deelnemersinformatie				
Werkgeversinformatie				
Website-informatie			1	
KvK				
Kosten	2	2	1	Zowel administratie als vermogensbeheer
Jaarrekening			1	
Geldstromen				In- en excasso
Deelnemersgegevens	3	1	2	Met name beschikbaar voor medewerkers van pensioenuitvoerder
Persoonsgegevens				
Financiële gegevens				Belastinginformatie
Dienstverbanden				
Arbeidsongeschiktheid		2		
Partner(s) en kinderen				
Uitkeringen		2		
Aanspraken				
Bankgegevens		2		
Werkgeversgegevens	2	2	2	Met name beschikbaar voor medewerkers van pensioenuitvoerder
NAW				
Loonheffingsnummer				
Bankrekeningnummer				
Incasso informatie				
KvK				
Beleggingsgegevens	2	2	2	Met name beschikbaar voor medewerkers van vermogensbeheerders, fiduciair en beleggingsadviseur
Beleggingsbeleid				
Strategisch/Tactisch				
Overeenkomsten				
Mandaten				

Bijlage 2: DNB Toetsingskader Informatiebeveiliging 2019-2020

Governance	
1	**Define an information security plan**
1.1	Information security plan
1.2	IT policies management
2	**Define the information architecture**
2.1	Enterprise Information architecture model
2.2	Data classification scheme
3	**Determine technological direction**
3.1	Monitor future trends and regulations
3.2	Technology standards
4	**Assess and manage (IT) risks**
4.1	IT risk management framework
4.2	Risk assessment
4.3	Maintenance and monitoring of a risk action plan
Organisation	
5	**Information security organization**
5.1	Responsibility for risk, security and compliance
5.2	Management of information security
6	**Data and system ownership**
6.1	Data and system ownership
7	**Manage segregation of duties**
7.1	Segregation of duties
People	
8	**Manage IT human resources**
8.1	Personnel recruitment and retention
8.2	Personnel competences
8.3	Dependence upon individuals
8.4	Personnel clearance procedures
8.5	Job change and termination
9	**Ensure operations and use**
9.1	Knowledge transfer to end users
9.2	Knowledge transfer to operations and support staff
9.3	Employee awareness
Processes	
10	**Change Management**
10.1	Change standards and procedures
10.2	Impact assessment, prioritisation and authorisation
10.3	Test environment
10.4	Testing of changes
10.5	Promotion to production
11	**Continuity Management**
11.1	IT continuity plans
11.2	Testing of the IT continuity plan
11.3	Offsite backup storage

11.4	Backup and restoration
12	**Manage data**
12.1	Storage and retention arrangements
12.2	Disposal
12.3	Security requirements for data management
13	**Configuration Management**
13.1	Configuration repository and baseline
13.2	Identification and maintenance of configuration items
14	**Manage third party and supplier services**
14.1	Monitoring and reporting of SLA's
14.2	Supplier risk management
15	**Incident Management**
15.1	Security incident definition
15.2	Incident escalation
16	**Monitoring**
16.1	Security testing, surveillance and monitoring
16.2	Monitoring of internal control framework
16.3	Internal control of third parties
16.4	Evaluation of compliance with external requirements
16.5	Independent assurance
17	**User account management**
17.1	Identity management
17.2	User account management
Technology	
18	**Secure infrastructure**
18.1	Infrastructure resource protection and availability
18.2	Infrastructure maintenance
18.3	Cryptographic key management
18.4	Network security
18.5	Exchange of sensitive data
19	**Manage malware attacks**
19.1	Malicious software prevention, detection and correction
19.2	Vulnerability management (Newly identified vulnerabilities)
19.3	Life cycle management
20	**Protect infrastructure components**
20.1	Protection of security technology
Facilities	
21	**Physical security**
21.1	Physical security measures
21.2	Physical access
Testing	
22	**Testing**
22.1	Penetration testing and ethical hacking