Stichting Pensioenfonds Forbo

IT Beleid
Bijlage R bij ABTN

December 2018
Dit document heeft 8 pagina’s

Versiebeheer

Versie	Auteur	Datum	Revisie
V1.0	Bestuur	18 december 2018	Nieuwe bijlage

Inhoudsopgave

1. Inleiding

In dit document wordt het IT beleid van Stichting Pensioenfonds Forbo (verder: het fonds) beschreven. Het IT beleid heeft betrekking op de kritieke processen die te maken hebben met IT risico's van zowel de eigen organisatie als de organisatie van de partijen waaraan werkzaamheden zijn uitbesteed, en heeft ten doel te voorkomen dat deze processen IT risico's bevatten die het fonds als ongewenst beschouwd.

2. Scope van het IT Beleid

Informatietechnologie wordt in veel onderdelen van de processen van het fonds gebruikt, en derhalve is het IT risico een belangrijk risico voor het fonds.
Omdat het fonds alle processen die te maken hebben met deelnemers- en pensioenadministratie, vermogensbeheer en beleggingsadministratie, actuariële berekeningen, actuarieel advies, en communicatie inclusief externe website heeft uitbesteed, wordt derhalve automatisch de opvolging en controle rond het IT risico een onderdeel van het uitbestedingsbeleid.

Het IT risico is een van de categorieën in de door de DNB gehanteerde toezichtaanpak "FIRM" en "Focus!". Het fonds dient aantoonbaar in control te zijn op het gebied van IT risico, en daarom wordt het beleid hierover apart behandeld in dit document. Dit beleid wordt vastgesteld door het bestuur van het fonds. En met de externe partijen waaraan werkzaamheden/processen zijn uitbesteed, besproken.

De eigen interne organisatie van Pensioenfonds Forbo draait volledig op de apparatuur en IT-infrastructuur van de sponsor Forbo. Daarom zijn het IT-beleid en de interne beheersingsprocessen van Forbo ook van toepassing op de interne processen van het fonds. Het fonds heeft vastgesteld dat deze processen en uitgangspunten in lijn zijn de IT-beleidsuitgangspunten van het fonds. .

3. IT risico's

IT risico's vallen uiteen in een aantal categorieën:
a. Bewustwording (Awareness)
b. Beschikbaarheid (Availability)
c. Toegang (Access)
d. Accuraatheid (Accuracy)
e. Flexibiliteit (Agility)

Daarbij kan gedacht worden aan:
- Onopzettelijke fouten in het ontwerp, gebruik of onderhoud van en aan IT systemen. Dit kan te maken hebben met IT netwerken, IT hardware,

software, management processen in de aansturing of besluitvorming met betrekking tot IT systemen;
- Fraude en andere risico's die het gevolg zijn van opzettelijke frauduleuze menselijke handelingen, zoals cybercrime;
- Omgevingsrisico's, zoals terrorisme, natuurrampen, of andere wijzigingen in de omgeving van IT systemen, waardoor deze niet meer naar behoren werken;
- Failissement van de uitbestedingsorganisatie of de eigen organisatie.

4. Beleidsuitgangspunten

Het fonds hanteert bij het IT beleid de volgende uitgangspunten:
- Het bestuur van het fonds is eindverantwoordelijk voor de IT activiteiten of -processen. Dit betekent dat het bestuur zicht moet hebben op de IT gerelateerde onderdelen van de uitvoering, ook bij uitbesteding van diensten en processen aan derde partijen en de processen bij de interne organisatie van de sponsor;
- Het IT beleid is van toepassing op alle bestaande-, voorgenomen nieuwe- of gewijzigde uitvoeringen of uitbestedingen;

De uitgangspunten in de overeenkomst tot uitbesteding zullen steeds corresponderen met de voorwaarden van het beleid.

5. Beleidsdoelstellingen

Het fonds wenst met het IT beleid zeker te stellen dat de informatievoorziening voldoet aan de volgende aandachtspunten:

a. Bewustwording (Awareness) in de zin dat alle werknemers en gebruikers in de organisatie zich bewust zijn van het belang van IT controles en zich voegen naar de IT richtlijnen.
b. Beschikbaarheid (Availability) in de zin van het draaien van bestaande processen, snel herstellen van storingen en het minimaliseren van de negatieve gevolgen van incidenten, zoals het niet beschikbaar zijn van systemen of van veiligheidslekken.
c. Toegang (Access) in de zin dat de juiste stafmedewerkers (middels beveiligingscodes) toegang hebben tot de juiste informatie en dat anderen dat niet hebben.
d. Accuraatheid (Accuracy) in de zin dat informatie accuraat, tijdig en volledig is voor alle relevante partijen.
e. Flexibiliteit (Agility) in de zin dat het mogelijk moet zijn om wijzigingen aan te brengen in bestaande systemen en processen, als dat noodzakelijk is voor de continue ondersteuning van een veranderende bedrijfsvoering bij het fonds, en dat het mogelijk is deze te implementeren tegen acceptabele kosten en binnen redelijke tijdlijnen.

Speciale aandacht wordt verwacht bij deze punten voor de processen die de directe invloedsferen van de partijen overstijgen, zoals cloud computing, websites en netwerken naar externe partijen.

6. Uitvoering van beleid en monitoring

De uitvoering van het beleid ligt bij het bestuur van het fonds. Het bestuur wordt daarbij geadviseerd door (externe) adviseurs. Het bestuur volgt de te nemen acties op en monitort de voortgang via de actielijst van de bestuursvergaderingen. Daarnaast worden IT risico's specifiek behandeld en beoordeeld in de risicocommissie.

(1) Het bestuur draagt er zorg voor dat de IT beleidsdoelstellingen van het fonds een integraal onderdeel zijn van de IT-organisatie van de sponsor en van de contracten en Service Level Agreements (SLA's) met de uitvoerende partijen.

(2) Het bestuur draagt er zorg voor dat bij de keuze van uitvoerder/ dienstverlener aan de IT beleidsdoelstellingen van het fonds wordt geconformeerd.

(3) In de SLA's ligt onder andere vast wat de afspraken zijn met betrekking tot de omgang met incidenten, de beschikbaarheid (continuïteit) van de systemen, hoe dit wordt gemonitord en hoe hierover gerapporteerd wordt.

(4) Verschillende aspecten zoals genoemd in de IT beleidsdoelstellingen worden meegenomen in de periodieke behandeling van de SLA rapportages. Andere aspecten worden behandeld in de jaarlijkse behandeling van de ISAE3402 rapportages van de uitbestedingspartijen en de performancerapportages, inclusief de resultaten van de jaarlijkse interne audit, van de sponsor. Deze behandeling vindt zowel binnen het bestuur als binnen de risicocommissie plaats.

(

5) De uitvoerende partijen wordt gevraagd naar de lange-termijn strategie op IT beleid, en specifiek naar de verschillende aspecten rond cloud computing, netwerkbeheer en websites.

Het bestuur draagt er zorg voor dat de uitvoering van het IT beleid zich op acceptabel niveau bevindt, dat samenhangt met de grootte en complexiteit van het fonds.

Dat wil zeggen:

- Formele controle is aanwezig voor de kritische processen.
- Kritische processen en controles zijn geselecteerd op basis van risicoanalyse.
- Er is documentatie aanwezig van de uitvoering van de controles.
- Er is documentatie aanwezig die "test of operating effectiveness" aantoont.
- "Test of operating effectiveness" (ISAE3402 en SLA review) wordt herhaald afhankelijk van het risicoprofiel.
- De periodieke evaluatie van de controles (scope van de ISAE3402 en SLA rapportages) is gedocumenteerd, inclusief acties die hier uit volgen.
- Er is periodieke rapportage over (onder-)uitbestedingspartners waaraan processen zijn uitbesteed, inclusief vermelding of dit om cloud-toepassingen gaat.
- De periodieke evaluatie van de controles wordt herhaald afhankelijk van het risicoprofiel, maar minimaal jaarlijks.

Bij de jaarlijkse risico-analyse wordt ook het IT risico geëvalueerd. Hierbij maakt het fonds gebruik van algemeen geaccepteerde procedures en aanbevolen check lists. De risico's worden gecategoriseerd in menselijke, technische en omgevingsrisico's, zoals aanbevolen door De Nederlandsche Bank en de Pensioenfederatie.

7. Inwerkingtreding en evaluatie IT beleid

Het IT beleid is vastgesteld in de vergadering van het bestuur van 18 december 2018. Het IT beleid wordt tweejaarlijks geëvalueerd en zonodig bijgesteld.