Bijlage bij het Informatiebeveiligingsbeleid:

Het End-user computingbeleid

Bpf Beton

Versie: december 2021

Inhoud

1. End-user computingbeleid

In dit document is het end user computingbeleid van Bpf Beton vastgelegd. Dit document betreft een aanvulling op en moet gezien worden als bijlage bij het Informatiebeveiligingsbeleid. In dit beleidsdocument is het IT-beleid verankerd.

1.1 Wat is end-user computing?

Pensioenfondsen en haar uitbestedingsrelaties werken regelmatig met rapportages, analyses en/of oplossingen die zijn ontwikkeld door middel van eigen applicaties en of oplossingen in Microsoft Office. Dit kan variëren van eenvoudige Word- of PowerPoint-sjablonen, tot zeer complexe Excel-analyses of complexe Access-databases. Dit noemen we ook wel End-user computing.

End-user computing (hierna: "EUC") verwijst naar systemen waarin niet-programmeurs werktoepassingen kunnen maken. EUC is een groep benaderingen van informatica die gericht is op een betere integratie van eindgebruikers in de computeromgeving.

1.2 Noodzaak EUC-beleid

EUC-toepassingen worden voor verschillende doeleinden ingezet. Denk bijvoorbeeld aan de adviserend actuaris of de pensioenadministrateur die vaak financiële beslissingen op automatische berekeningen en analyses in spreadsheets baseren. Het gebruik van EUC-toepassingen heeft zich ontwikkeld van eenvoudige spreadsheets tot geavanceerde en ingewikkelde actuariële analyses.

Het grote voordeel van EUC is dat gebruik en het ontwikkelen van oplossingen snel en goedkoop is. Het nadeel van EUC-toepassingen is dat deze vaak lastig te onderhouden zijn en ontwikkeld zijn zonder na te denken over het aantoonbaar borgen van de juistheid, volledigheid en tijdigheid van de data. Dit omdat ze vaak buiten scope van IT-beheersingsprocessen vallen en daarmee ook niet formeel in beheer worden genomen door de IT-organisatie.

Verder zijn zaken zoals de continuïteit en documentatie niet geborgd. Dit sluit niet aan bij de beheersingseisen zoals deze in het IT-beleid gesteld staan.

Dit resulteert in een groot risico voor de organisatie en de gebruikers van deze tools, die vaak afhankelijk zijn van de goede werking van deze EUC-toepassingen bij het maken van de juiste, op feiten gebaseerde operationele of beslissingen. Om deze redenen is het noodzakelijk om een EUC-beleid op te stellen.

1.3 Doel van het EUC-beleid

Het EUC-beleid is onderdeel van het IT-beleid van Bpf Beton en moet op integrale wijze worden bezien. Met het IT-beleid wil het bestuur de belanghebbenden, uitbestedingspartijen en overige partijen van het fonds inzicht geven in het gevoerde IT-beleid en de wijze van beheersing van de IT-risico's. In het IT-beleid worden tevens specifieke eisen gesteld aan de datakwaliteit middels een BIV-classificatie. Een BIV-classificatie of indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de beschikbaarheid, de integriteit en de vertrouwelijkheid van informatie en systemen wordt aangegeven. Het IT-beleid heeft als één van de belangrijkste doelen om datakwaliteit te borgen. Dat uit zich in het tijdig, juist en volledig beschikbaar hebben van data.

Het EUC-beleid heeft als doel: het bestuur, de belanghebbenden, uitbestedingspartijen en overige partijen van het fonds inzicht te geven in het gevoerde beleid en de wijze van beheersing van de IT-

risico's bij het gebruik van end user computing.

Met dit beleid wil het bestuur de belanghebbenden, medewerkers, uitbestedingspartijen en overige partijen van het fonds inzicht geven in het gevoerde informatiebeveiligingsbeleid en de wijze van beheersing van de risico's ten aanzien van EUC. Dit beleid is ingegeven door:

1. De eis van een beheerste en integere bedrijfsvoering, volgend uit artikel 143 van de Pensioenwet en artikel 18 van het Besluit financieel toetsingskader pensioenfondsen. Dit houdt onder meer in dat het fonds moet beschikken over procedures, maatregelen en systemen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen. Hierbij is de integrale samenhang met andere beleidsgebieden en risico's van essentieel belang;
2. De noodzaak van het compliant zijn van de wijze van verwerking van persoonsgegevens met de Algemene Verordening Gegevensbescherming (AVG), waarin is geregeld dat er sprake moet zijn van een set aan passende technische- en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking;
3. De visie van het bestuur dat de mate van digitalisering en de snelheid waarmee dit plaatsvindt enerzijds positieve effecten kan hebben (bijvoorbeeld in de vorm van te realiseren kostenbesparingen en geautomatiseerde controlefuncties) maar anderzijds ook tot bedreigingen kan leiden (bijvoorbeeld cybercrime, datalekken en onbeheersbaarheid van de volledige IT-infrastructuur).

Zowel de eigen IT-omgeving als iedere uitbestedingspartij dient te voldoen aan IT-beheersingsnormeringen.

1.4 Uitgangspunten bij gebruik van EUC

In termen van risico's van de datakwaliteit betekent end-user computing een hoger risico op fouten. EUC geeft risico's door de beperkingen en zwakke punten door wanneer het gaat om loggen van mutaties, het verwerken van grote hoeveelheden data, versie beheer, het ontbreken van een beheerst ontwikkel- en testproces en het kunnen inrichten van een beheerst autorisatiemanagement. Daarom zijn de volgende uitgangspunten belangrijk:

1. Als uitgangspunt geldt dat het gebruik van EUC in beginsel moet worden beperkt tot die processen waarbij een hoge mate van flexibiliteit wenselijk of noodzakelijk is, zoals het analyseren en aansluiten van gegevens;

2. Indien er redelijke alternatieven bestaan voor het gebruik van EUC, dan zullen deze moeten worden overwogen met het oog op een verbetering van de beheersing van de datakwaliteit. Hierbij doelen wij op het beheersen van de juistheid, tijdigheid en volledigheid van de data alsook de bescherming van privacy en het voorkomen van ongeautoriseerd gebruik van data.

1.5 Beheersing van EUC

Voor zover EUC onvermijdelijk is moet voorafgaand aan de ontwikkeling en het gebruik in de pensioenuitvoering nadere eisen worden gesteld in het geval dat EUC kritisch is voor het pensioenuitvoeringsproces. Dit wordt hieronder nader uiteengezet.

Het bestuur hanteert ten aanzien van de beheersing een gelaagde aanpak:

1. Hierbij wordt bewust onderscheid gemaakt tussen fondskritische en niet-fondskritische uitbestedingspartijen, waarbij het bestuur zich baseert op de uitkomsten van de IT-risicoanalyse. Bij de vaststelling van dit beleid per gelden de volgende uitbestedingspartijen als fondskritisch:
    i. Pensioenadministratie BPF Beton (Centric)
    ii. Fiduciair / vermogensbeheer (BMO)
    iii. Actuariële werkzaamheden (Centric en WTW)

    De volgende processen zijn als ondersteunend geclassificeerd:
    iv. Bestuursondersteuning (Centric)
    v. Jaarverslaggeving (Centric)
    vi. Jaarwerkcontrole (BDO, WTW en Centric)

2. Per fondskritische uitbestedingspartij brengt het bestuur in samenwerking met de desbetreffende uitbestedingspartij in kaart of en voor welke processen van EUC gebruik wordt gemaakt.
3. Op basis van de van de uitbestedingspartijen ontvangen reacties beoordeelt het bestuur welke EUC-gekoppelde processen als risicovol (volgens de “hoog / midden / laag-methodiek”) moeten worden beschouwd Essentiële criteria hierbij zijn:
    a. De datakwaliteit. Hierdoor kunnen bijvoorbeeld fouten in de pensioenuitvoering ontstaan of foutieve bestuurlijke besluiten worden genomen;
    b. Het toegankelijk zijn van informatie voor ongeautoriseerden;
    c. Kan op een inbreuk op de privacy van betrokkenen;
    d. Kan een onjuist beeld geven van beleggingsdata of andere financiële data op basis waarvan foutief beleid wordt geformuleerd, foutieve adviezen worden gegeven en/of foutieve bestuurlijke besluiten worden genomen.
4. Van de processen met een risicoclassificatie “hoog” of “midden” wordt de uitbestedingspartij gevraagd een Risk Self Assessment (RSA) en – indien van toepassing – een Privacy Impact Assessment (PIA) – aan te leveren (of indien deze nog niet beschikbaar is, als nog uit te voeren). Dit is overeenkomstig van toepassing op EUC-processen die voor het eerst worden geïmplementeerd en gebruikt.

Belangrijk aandachtspunt:
Indien EUC kritisch is en/of langere tijd ingezet gaat worden, dan wenst het bestuur hierover schriftelijk geïnformeerd en gerapporteerd te worden. Niet alleen voorafgaand aan het inzetten hiervan maar ook tijdens het gebruik hiervan. Verder ontvangen zij graag de resultaten van de uitgevoerde RSA en PIA.

1.6 Eisen aan het ontwerp en ontwikkeling van de EUC-oplossing

Het ontwikkelen van een kritische EUC moet beheerst plaatsvinden volgens een gedefinieerd changemanagementproces. Het bestuur beoordeelt hierbij of de uitbestedingspartij de volgende uitgangspunten in acht heeft genomen en stelt op basis van de uitkomsten vast of hieraan is voldaan. Het bestuur behoudt zich in alle gevallen de mogelijkheid voor om in voorkomende gevallen een of meerdere uitgangspunten buiten beschouwing te laten.

- In het ontwerp van de kritische EUC-toepassingen worden invoer, bewerking en uitvoer zoveel mogelijk gescheiden;
- Formules, bewerkingen en uitvoervelden worden zoveel mogelijk beveiligd tegen ongeautoriseerd muteren;
- De EUC is alleen toegankelijk voor geautoriseerden;
- Iedere EUC is voorzien van een eigenaar;
- De EUC-toepassing wordt getest en bevat indien noodzakelijk controletotalen en verbandscontroles wat een indicator is voor de datakwaliteit;
- De EUC beschikt over een gebruikersinstructie en andere noodzakelijke beheersdocumentatie;
- De EUC wordt opgenomen in het configuratiemanagementproces en andere IT-beheersingsprocessen;
- De EUC wordt middels en heldere instructie en/of opleiding geïmplementeerd.
- Het ontwerp en de ontwikkeling van de EUC voldoen aan de eisen zoals gesteld in het changemanagementproces;
- Na het ontwikkelen van de EUC wordt deze getest. De proces- en/of tooleigenaar keurt de ingebruikname goed indien aan de test-, kwaliteits- en beheersingsnormen is voldaan;
- Om de datakwaliteit te borgen is het essentieel om EUC net als professionele IT-infrastructuur te beheersen. Iedere EUC dient daarom en verantwoordelijke te hebben en geïmplementeerd te zijn in het configuratiemanagementproces en andere beheersingsprocessen zoals autorisatiemanagement, changemanagement en incidentmanagement;
- Er is aantoonbaar versiebeheer aanwezig;
- Oude versies van EUC blijven beschikbaar in lijn met de gestelde bewaartermijnen zoals opgenomen in het archiefbeleid van het fonds;
- Er is een register aanwezig als onderdeel van het configuratiemanagement waaruit blijkt welke kritische EUC in gebruik zijn.

Belangrijk aandachtspunt:
Indien het niet mogelijk is om de EUC in beheer te nemen wenst het bestuur hierover geïnformeerd te worden. Daarbij ontvangt zij tevens een toelichting hoe de datakwaliteit geborgd blijft.

Er dient een register van EUC aanwezig te zijn waarin alle kritische EUC geregistreerd worden met versie en eigenaar welke in gebruik zijn. Dit overzicht moet ten allen tijden opvraagbaar kunnen zijn.

2. Vaststelling EUC-beleid

Dit aanvullende EUC-beleid is vastgesteld door het bestuur op 17 december 2021 en treedt in werking met onmiddellijke ingang.