Incidentenregeling

Stichting Pensioenfonds Ecolab

13 maart 2025

INCIDENTENREGELING

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van Stichting Pensioenfonds Ecolab.

Deze Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een Incident binnen het fonds. Doel van deze regeling is het beschermen van de organisatie door schade aan de integriteit, beheerste bedrijfsvoering en reputatie van het fonds te voorkomen en mogelijke gevolgschade te beperken. Deze regeling waarborgt een consistente en geïntegreerde monitoring, behandeling en opvolging van alle incidenten, met als doel onderliggende oorzaken te identificeren, te documenteren en weg te nemen om toekomstige incidenten te voorkomen.

Daarnaast wil het fonds leren van Incidenten om herhaling te voorkomen. Stichting Pensioenfonds Ecolab streeft er naar een betrouwbare, transparante en lerende organisatie te zijn. Daarbij past een cultuur waarin medewerkers Incidenten kunnen melden en waarin helder is hoe met deze melding zal worden omgegaan.

Vanaf 17 januari 2025 is de Digital Operational Resilience Act (DORA) van kracht. Waarmee aanvullende eisen zijn ingevoerd voor de digitale operationele weerbaarheid van Stichting Pensioenfonds Ecolab. Deze Incidentenregeling beschrijft het algemene beleid voor het melden, vastleggen en afhandelen van alle incidenten die de integere en beheerste bedrijfsvoering kunnen raken. In lijn met DORA zijn aan deze regeling specifieke procedures toegevoegd voor ernstige ICT-incidenten, die apart moeten worden geregistreerd, gemeld en opgevolgd. Artikel 17 van DORA verplicht het fonds tot een beheerproces voor ICT-incidenten, waarin dergelijke ernstige incidenten en significante cyberdreigingen systematisch worden vastgelegd.

Bij deze regeling hoort een ICT-incidentenprocedure. Deze ICT-incidentenprocedure gaat in op het beheerproces van ernstige ICT-incidenten. In de ICT-incidentenprocedure wordt ingegaan op de classificatieprocedure van deze incidenten en hoe deze gemeld worden aan de toezichthouder volgens de DORA-vereisten.

Met deze regeling geeft Stichting Pensioenfonds Ecolab mede uitvoering aan de vereisten van de Pensioenwet en de Code Pensioenfondsen inzake de omgang met en de vastlegging van Incidenten en ook aan de aanvullende eisen uit DORA. Hiermee wordt de digitale operationele weerbaarheid van het fonds versterkt, en worden de belangen van deelnemers beter beschermd tegen digitale verstoringen.

Artikel 1 - Definities

Toezichthouder	De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens, de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) Stichting Pensioenfonds Ecolab.
Incidenten	Een gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van Stichting Pensioenfonds Ecolab, en/of een gebeurtenis waarbij directe of indirecte financiële schade ontstaat door ontoereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen dan

	wel een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming. Er wordt een onderscheid gemaakt tussen Operationele Incidenten, ernstige ICT-incidenten en Overige Incidenten.
Operationele Incidenten	Een Incident dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door Stichting Pensioenfonds Ecolab en waarbij er een inbreuk is geweest op de beheerste bedrijfsvoering. Onder operationele Incidenten vallen ook de reguliere ICT-incidenten.
ICT-incident	Een incident dat betrekking heeft op de ICT-systemen van het fonds, waarbij de vertrouwelijkheid, authenticiteit, beschikbaarheid of integriteit van data in gevaar komt, of dat de bedrijfscontinuïteit verstoort, door bijvoorbeeld technische storingen, cyberaanvallen, rampen, ongeoorloofde toegang of uitval van systemen. Deze incidenten vormen een bedreiging voor de normale werking van de ICT-infrastructuur en vereisen een adequate respons om de schade te beperken.
Overige Incidenten	Alle Incidenten, die niet beschouwd kunnen worden als Operationele Incidenten of ernstige ICT-incidenten. Onder overige Incidenten worden in ieder geval verstaan: • een (dreigende) bewuste schending van wet- en regelgeving; • een (dreiging van) bewust onjuist informeren van publieke organen; • een (dreigende) schending van binnen de Stichting Pensioenfonds Ecolab geldende gedragsregels; • (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie over deze feiten. • een ernstig gevaar voor de integere bedrijfsuitoefening van Stichting Pensioenfonds Ecolab; • gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media; • fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van Verbonden persoon; • een (mogelijk) aanwijzing van een Toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen; • overige strafbare feiten.
Ernstig ICT-incident	Een ICT-incident dat een significant risico vormt voor de beheerste en integere bedrijfsvoering van het fonds en/of een ernstige bedreiging vormt voor de bedrijfscontinuïteit. Onder ernstige ICT-incidenten worden onder mee begrepen: omvangrijke cyberaanvallen, grote datalekken, langdurige uitval van kritieke systemen en verstoringen die een groot afbreukrisico kunnen opleveren voor de reputatie van het fonds. Voor ernstige ICT-incidenten geldt een specifieke meldings- en opvolgingsprocedure, conform de eisen die zijn vastgelegd in DORA.

Kritieke of belangrijke functie	Een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten.
Compliance Officer	De functionaris die als Compliance Officer is benoemd;
Verbonden personen	Een medewerker van Stichting Pensioenfonds Ecolab , onafhankelijk van de duur waarvoor of de juridische basis waarop hij werkzaam is; 2 Bestuurders van Stichting Pensioenfonds Ecolab 3 degenen die voor het pensioenfonds werkzaamheden verrichten maar niet bij het pensioenfonds in dienst zijn 4 Andere (categorieën) personen die zijn aangewezen door Stichting Pensioenfonds Ecolab als Verbonden persoon.
ICT-comité	Het ICT-comité bestaat uit het bestuurslid met integraal risico-management in portefeuille en het bestuurslid in de rol van NFR-risico-eigenaar (risk manager) ondersteunt door de extern ingehuurde Security Officer;
Risk manager	Deze rol is toegewezen aan het bestuurslid met als toegewezen rol NFR-risico eigenaren;
Security Officer	Deze rol is uitbesteed door het pensioenfonds aan een extern deskundige met juiste kennis op het gebied van ICT, cyber- en security risico's. Deze rol is vanaf 13 maart 2025 ingevuld door een vertegenwoordiger van Argis BV;
DORA	DORA is de Digital Operational Resilience Act, een verordening van de Europese Commissie die in werking treedt op 17 januari 2025.

Artikel 2 - Melden, beoordelen en vastleggen van Incidenten

1. Iedere Verbonden persoon die een (dreigend) Incident constateert is gehouden dit te melden aan de Compliance Officer. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem gedaan worden.

2. Als zich bij een partij waaraan werkzaamheden heeft uitbesteed een Incident voordoet, meldt deze uitbestedingsrelatie het Incident aan het dagelijks bestuur van het pensioenfonds. Dagelijks bestuur zorgt ervoor dat de melding tijdig aan de Compliance Officer wordt doorgegeven. Het Fonds draagt er zorg voor dat de uitbestedingsrelatie bekend is met deze regeling en weet bij wie een Incident gemeld moet worden.

3. De Compliance Officer is verantwoordelijk voor het beheren en het up-to-date houden van het incidentenregister. De Compliance Officer beoordeelt in samenwerking met het dagelijks bestuur de melding voorzover dit geen ICT-incident betreft. De Compliance Officer bepaalt of er sprake is van een Incident en zo ja, of er dan sprake is van een Operationeel dan wel een Overig Incident. Dit oordeel wordt vastgelegd. Wanneer blijkt dat het incident een ICT-incident is, moet worden beoordeeld of

het een ernstig ICT-incident is. Deze beoordeling wordt niet door de Compliance Officer uitgevoerd. Wel wordt de Compliance Officer op de hoogte gebracht van de uitkomst en inhoud van de beoordeling, zodat dit geregistreerd kan worden in het incidentenregister. Hoe ICT-incidenten worden beoordeeld staat in artikel 2a en de ICT-incidentenprocedure. Als blijkt dat het ICT-incident als niet ernstig wordt gekwalificeerd worden de stappen uit de Incidentenregeling gevolgd van incidenten, artikel 2, 3 en 4.

4. Meldingen van Incidenten en de beoordeling van de Compliance Officer van het Incident worden geregistreerd in het Incidentenregister. Gedurende het verdere proces worden in het dossier de naar het oordeel van de Compliance Officer relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek.

5. Incidentendossiers worden zodanig bewaard dat de vertrouwelijkheid wordt gewaarborgd in een beveiligde omgeving. Indien er sprake is van de betrokkenheid van een Verbonden persoon worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen de Compliance Officer en de voorzitter van het Fonds toegang hebben tot deze gegevens.

6. De Compliance Officer informeert de melder over zijn beoordeling zoals bedoeld in artikel 2.4. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

7. De melding en de daarbij beschikbaar gestelde gegevens worden door alle betrokken partijen strikt vertrouwelijk behandeld. De identiteit van de melder wordt niet opgenomen in communicatie naar derden tenzij daar een wettelijke verplichting toe bestaat.

8. Een ieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident, betracht daarover uiterste geheimhouding, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen. Indien voor de afronding van het Incident openheid van zaken is vereist, kan het bestuur beslissen dat de verplichting tot geheimhouding geheel of gedeeltelijk vervalt.

Artikel 2a – Melden, beoordelen en vastleggen van Ernstige ICT-incidenten

1. Voor het beoordelen van ernstige ICT-incidenten moet als eerste stap worden bepaald of ‘kritieke of belangrijke functies’ worden geraakt met het ICT-incident. Voor het fonds zijn de kritieke of belangrijke functies de volgende:
   - Uitvoeren pensioenadministratie
   - Incasso
   - Excasso

2. Wanneer een ICT-incident impact heeft op een kritieke of belangrijke functie wordt beoordeeld of het incident als ernstig moet worden aangemerkt. De eerste stap in deze beoordeling is het vaststellen of er sprake is van een succesvolle kwaadaardige, ongeautoriseerde toegang tot het netwerk en/of informatiesystemen (zoals bij ransomware of hacking). Indien dit het geval is kwalificeert het als een ernstig ICT-incident. Indien dit niet het geval is, wordt het incident verder beoordeeld aan de hand van zes aanvullende criteria. Als geen of slechts een van de criteria van toepassing is, wordt het incident als niet ernstig beschouwd. Indien echter twee of meer criteria worden geraakt, wordt het incident aangemerkt als een ernstig ICT-incident.

3. Bovenstaande procedure, inclusief classificatieproces en zes criteria zijn verder uitgewerkt in de ICT-incidentenprocedure Pf Ecolab.

4. Het ICT-comité bepaalt de impact van het incident door middel van de classificatie en criteria uit de DORA verordening. Het bestuur blijft eindverantwoordelijk voor de ernstige ICT-incidenten. Het ICT-comité registreert en classificeert het incident met informatie van het ICT-incident en neemt de benodigde stappen conform de DORA vereisten.

5. Als blijkt dat er sprake is van een ernstig ICT-incident, dient er een eerste kennisgeving te worden gerapporteerd aan DNB. Deze eerste kennisgeving van het ernstige ICT-incident wordt opgevoerd via het

"MijnDNB"-portaal, het fonds is hier verantwoordelijk voor.

6. De eerste kennisgeving moet binnen 4 uur na de classificatie als ernstig ICT-incident worden gemeld bij DNB en niet later dan 24 uur na het moment dat het fonds kennis heeft genomen van het incident. Het ICT-comité houdt de deadline voor het aanleveren van de eerste kennisgeving in de gaten. De eerste kennisgeving wordt opgesteld met behulp van de ICT-incidentenprocedure.

7. Het ICT-comité neemt gedurende het verdere proces in het dossier de relevante documenten op, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek. Het ICT-comité noteert alle stappen die worden genomen tijdens de incidentafdeling voor het eindverslag. Het eindverslag moet worden aangeleverd als afronding van een ernstig ICT-incident. Dit wordt behandeld in artikel 4a van deze Incidentenregeling.

Artikel 3 - Behandeling van Incidenten

1 Indien de Compliance Officer van mening is dat er sprake is van een Operationeel Incident brengt hij de leidinggevende van de afdeling waar zich het Operationeel Incident heeft voorgedaan op de hoogte. Indien de Compliance Officer van mening is dat er sprake is of kan zijn van een Overig Incident brengt hij het Bestuur op de hoogte. Door de voorzitter van het Bestuur wordt, na advies van de Compliance Officer, besloten of en wanneer andere organen van het Fonds, sleutelfunctiehouders en/of overige belanghebbenden op de hoogte moeten worden gebracht van het Incident.

2 De afdeling waar zich het Operationele Incident heeft voorgedaan behandelt het Operationele Incident. De leiding gevende coördineert de afhandeling van het Operationele Incident met ondersteuning van de het ICT-Comité en/of Compliance Officer.

3 De Compliance Officer behandelt de Overige Incidenten, tenzij het Bestuur, na advies van de Compliance Officer, besluit dat, gelet op de aard of achtergronden van het Overige Incident, afwikkeling door een andere functionaris of een speciaal daarvoor te benoemen Onderzoekscommissie de voorkeur geniet. Een Onderzoekscommissie kan bestaan uit medewerkers van het fonds en/of externe deskundigen

4. Als een onderzoek wordt verricht door een andere persoon dan de Compliance Officer of door een Onderzoekscommissie, is/zijn de onderzoeker(s) gehouden de Compliance Officer op de hoogte te brengen en te houden van alle ontwikkelingen in het onderzoek vanwege zijn coördinerende en registrerende rol.

5. De Compliance Officer bewaakt de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties en rapporteert hierover aan het Bestuur.

Artikel 3a – Behandeling van ernstige ICT-incidenten

1. Het ICT-comité houdt toezicht op de behandeling van ernstige ICT-incidenten. Binnen het pensioenbureau moet het incident worden afgehandeld en passende maatregelen worden genomen, zodat het incident niet nogmaals voorkomt. Het bestuur kan samen met het ICT-comité ervoor kiezen om een Onderzoekscommissie hiervoor te benoemen. Een Onderzoekcommissie kan bestaan uit medewerkers van het fonds en/of externe deskundigen. Stichting Pensioenfonds Ecolab moet voldoende informatie verzamelen over het incident om een tussentijdsverslag op te kunnen stellen.

2. Binnen 72 uur na de eerste kennisgeving moet er een tussentijdsverslag worden aangeleverd bij DNB. Tevens dient er een tussentijdsverslag aangeleverd te worden na een ingrijpende wijziging van de status van het oorspronkelijke ernstige ICT-incident of nadat de behandeling van het incident is gewijzigd op basis van beschikbare nieuwe informatie. Het ICT-comité houdt de deadline voor het aanleveren van het tussentijdsverslag in de gaten.

3. Het tussentijdsverslag wordt opgesteld met behulp van de ICT-incidentenprocedure. Het fonds is

verantwoordelijk om de melding te doen via het “MijnDNB”-portaal.

Artikel 4 – Afronding van Incidenten

Na de behandeling van elk Incident wordt, ter afronding, door Stichting Pensioenfonds Ecolab besloten of er maatregelen genomen dienen te worden. De genomen maatregelen zullen zijn gebaseerd op de aard van het Incident en de daaruit voortvloeiende gevolgen. De maatregelen kunnen onder meer zijn gericht op het beheersen en beperken van het optredende risico, het bevestigen van geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – van het Incident om herhaling in de toekomst te voorkomen. De eindverantwoordelijkheid voor de afronding van het Incident en de eventuele getroffen maatregelen ligt bij het Bestuur.

Artikel 4a – Afronding van ernstige ICT-incidenten

1. Na de behandeling van een ernstig ICT-incident wordt, ter afronding, door Stichting Pensioenfonds Ecolab besloten of er maatregelen genomen dienen te worden. De maatregelen zijn gebaseerd op de aard van het incident en de daaruit voortvloeiende gevolgen. De maatregelen zijn onder meer gericht op het beheersen en beperken van het ernstige ICT-incident.

2. Naast het intern oplossen van het ernstige ICT-incident dient er over het incident een eindverslag te worden aangeleverd bij DNB. Dit eindverslag moet binnen een maand na de laatste update van het tussentijdsverslag worden aangeleverd. Het ICT-comité houdt de deadline voor het aanleveren van het eindverslag in de gaten. De eindverantwoordelijkheid voor de afronding van het ernstige ICT-incident en de eventuele getroffen maatregelen ligt bij het bestuur. Het eindverslag wordt opgesteld met behulp van de ICT-incidentenprocedure. Het fonds is verantwoordelijk om de melding te doen via het “MijnDNB”-portaal.

3. Stichting Pensioenfonds registreert ernstige ICT-incidenten in het incidentenregister, dat tevens als input dient voor het jaarlijkse evaluatieverslag dat Stichting Pensioenfonds Ecolab volgens DORA opstelt en indient bij de toezichthouder. In dit verslag wordt het kader voor ICT-risicobeheer geëvalueerd en worden alle relevante ICT-incidenten opgenomen. Naast de jaarlijkse rapportage wordt het verslag ook bijgewerkt bij ernstige ICT-incidenten of op verzoek van de toezichthouder, om zo de operationele weerbaarheid van het fonds te waarborgen.

Artikel 5 - Rapportage

1. De voortgang van de afhandeling van Incidenten wordt in de vergadering van het Bestuur geagendeerd. Het Bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het Bestuur kunnen de Compliance Officer en/ of het Management toezien op de daadwerkelijke opvolging.

2. In de rapportage(s), zoals die periodiek aan het Bestuur worden aangeboden, wordt inzicht gegeven in het aantal Incidenten dat zich de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de afhandeling van Incidenten en naar aanleiding van deze Incidenten genomen maatregelen.

Artikel 6 – Spoedeisend belang

1. Indien de aard van het Incident snel handelen vereist is de Voorzitter, of diens plaatsvervanger, bevoegd om namens het Bestuur een (voorlopig) besluit te nemen over de afhandeling van het Incident.

2. De Voorzitter is gehouden om de overige leden van het Bestuur zo snel mogelijk op de hoogte te brengen van de door hem verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het Bestuur aan te bieden.

Artikel 7 - Melden toezichthouder en overige communicatie

1. Door of namens het Bestuur wordt onverwijld de relevante Toezichthouder over een Incident geïnformeerd als er sprake is van een Incident dat een ernstig gevaar vormt voor de beheerste en integere bedrijfsvoering. Hiervan is in ieder geval sprake als:
   - aangifte is of wordt gedaan bij justitiële autoriteiten;
   - het voortbestaan van Stichting Pensioenfonds Ecolab wordt bedreigd of zou kunnen worden bedreigd;
   - er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere bedrijfsvoering door het Fonds;
   - mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het Fonds;
   - of de ernst, de omvang of de overige omstandigheden van het Incident in aanmerking genomen, de Toezichthouder in verband met haar toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.
   - Er sprake is van een ernstig ICT-incident dat valt onder de DORA verordening. In dit geval gelden afwijkende termijnen zoals vastgelegd in deze Incidentenregeling. Wanneer blijkt dat Stichting Pensioenfonds Ecolab de deadlines voor de eerste kennisgeving, tussentijdsverslag en eindverslag niet halen zullen zij tijdig DNB op de hoogte stellen en bij DNB aangeven wanneer zij wel de rapportages zullen indienen. Als de deadlines vallen in het weekend mogen de rapportages worden ingediend op de eerstvolgende werkdag voor 12:00.

2. De Toezichthouder zal op de hoogte worden gebracht van alle feiten, omstandigheden en achtergronden van het Incident, alsmede de maatregelen die naar aanleiding van het Incident zijn genomen of nog worden genomen.

3. Het Bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten. Door het Bestuur wordt, na advies van de Compliance Officer of ICT-comité, besloten of en wanneer andere organen van het Fonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een Incident.

Artikel 8 - Omgang met meldingen

1. Stichting Pensioenfonds Ecolab gaat er altijd van uit dat een melding van een Incident te goeder trouw is gedaan, tot het moment dat zij overtuigd is geraakt van het tegendeel.

2. Stichting Pensioenfonds Ecolab draagt er zorg voor dat een melder, ongeacht de wijze waarop hij melding heeft gemaakt van een Incident, op geen enkele wijze in zijn positie bij Stichting Pensioenfonds Ecolab benadeeld wordt, voor zover te goeder trouw gehandeld is.

3. Stichting Pensioenfonds Ecolab draagt er zorg voor dat niemand wordt benadeeld in zijn of haar positie bij Stichting Pensioenfonds Ecolab vanwege het uitoefenen van de taken en/of verplichtingen uit deze regeling.

4. In geval van intrekking van een melding zal Stichting Pensioenfonds Ecolab, ongeacht de wijze waarop melding is gemaakt van een Incident, zich ervan vergewissen dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

5. Een Verbonden persoon die willens en wetens heeft deelgenomen aan of veroorzaker is van een Incident, zal bij melding van dit Incident geen recht kunnen ontlenen aan de beschermingsregels zoals die gelden voor een te goeder trouw handelende Verbonden persoon.

Artikel 9 - Klokkenluidersregeling

1. Het Fonds beschikt tevens over een Klokkenluidersregeling. Deze regeling is van toepassing bij (een vermoeden van) een misstand. De definitie van een (vermoeden van) een misstand is opgenomen in de Klokkenluidersregeling. Indien een gebeurtenis kwalificeert als een misstand, dan kan de Verbonden persoon de procedure zoals beschreven in de Klokkenluidersregeling volgen

Artikel 10 - Overig

Deze regeling is door het bestuur vastgesteld op 13 maart 2025 en treedt direct in werking onder gelijktijdige intrekking van de bestaande Incidentenregeling.