Incidentenregeling
van
Stichting Pensioenfonds Mediahuis Nederland

Versie	Datum inwerkingtreding	Gewijzigd door	Samenvatting wijzigingen
8.1	December 2024	Paul de Koning	Update i.v.m. invoering DORA
8.2	September 2025	Paul de Koning	Jaarlijkse evaluatie / update beleid

Artikel 1: Definities

Pensioenfonds	Stichting Mediahuis Nederland Pensioenfonds.
Toezichthouder	De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) het pensioenfonds.
Incident	Een gebeurtenis die een (ernstig) gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het pensioenfonds 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 majeur IT incident zoals gedefinieerd in de wetgeving DORA of een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming.

Onder 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 het pensioenfonds geldende gedragsregels;
- (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie over deze feiten;
- een ernstig gevaar voor de integere bedrijfsuitoefening van het pensioenfonds;
- gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media;
- fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in de 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.

Er wordt een onderscheid gemaakt tussen Integriteitsincidenten, Beveiligingsincidenten, Operationele Incidenten, Overige Incidenten en een majeur IT incident volgens DORA.

Integriteitsincident	Een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende organisatie.
Operationeel Incident	Een Operationeel Incident is een gebeurtenis die plaatsheeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het pensioenfonds en waarbij er een inbreuk is geweest op de bedrijfsvoering.
Beveiligingsincident	Inbreuk op de beveiliging, waarbij de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie in gevaar is of kan komen. Bijvoorbeeld: • het kwijtraken of de diefstal van een USB-stick, dvd of cd-rom; • het kwijtraken of de diefstal van een laptop, smartphone of tablet; • een directory die een heel weekend per ongeluk heeft opengestaan; • een calamiteit zoals een brand of inbraak in het datacentrum; • een cyberaanval.
Overige incidenten	Alle Incidenten, die niet beschouwd kunnen worden als Integriteits-incidenten, Beveiligingsincidenten of Operationele Incidenten.
Majeur IT incident Onder de wetgeving DORA	Wanneer een IT incident als ernstig (Majeur) wordt geclassificeerd. Deze incidenten worden apart In deze regeling benoemd aangezien ze ook gemeld moeten worden bij de toezichthouder.
Compliance Officer	Degene die verantwoordelijk is voor het uitvoeren van de compliance werkzaamheden.

Verbonden Personen	Een medewerker van het pensioenfonds onafhankelijk van de duur waarvoor of de juridische basis waarop deze persoon werkzaam is; Bestuurders van het pensioenfonds; Andere (categorieën) personen die in de Gedragscode zijn aangewezen door het pensioenfonds als Verbonden persoon.

Artikel 2: Melden, beoordelen en vastleggen van Incidenten

2.1. Iedere Verbonden persoon die een (vermoeden van een) Incident constateert is gehouden dit te melden aan de directeur van het Pensioenfonds. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem gedaan worden. Het dagelijks bestuur wordt door de directeur van het Pensioenfonds op de hoogte gebracht. De Compliance Officer zal periodiek, minimaal 1 keer per jaar, het incidentenregister inzien.

2.2. Als zich bij een partij waaraan het Pensioenfonds werkzaamheden heeft uitbesteed een Incident voordoet, meldt deze uitbestedingsrelatie het Incident aan de directeur van het Pensioenfonds. De directeur van het Pensioenfonds draagt er zorg voor dat de uitbestedingsrelatie bekend is met deze regeling en weet bij wie een Incident gemeld moet worden.

2.3. Het staat een Verbonden persoon vrij een (een vermoeden van een) Incident ook aan de Compliance Officer te melden.

2.4. Het dagelijks bestuur beoordeelt de melding en overlegt deze met de Compliance Officer, waarna wordt bepaald of er sprake is van een Incident en zo ja, of er dan sprake is van een Operationeel Incident, Beveiligingsincident, Integriteitsincident, majeur IT incident of een Overig Incident. Dit oordeel wordt vastgelegd.

2.5. Meldingen door verbonden personen van Incidenten en de beoordeling van het Incident worden geregistreerd in het (IT) Incidentenregister, tenzij de gevoeligheid van de informatie een dergelijke registratie in de weg staat. Gedurende het verdere proces worden in het dossier de naar het oordeel van het dagelijks bestuur en Compliance Officer relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel (extern uitgevoerd) onderzoek.

2.6. IT-incidenten worden door het dagelijks bestuur geclassificeerd en gecommuniceerd aan de compliance officer waarna de informatiemanager het incident opneemt in het (IT) incidentenregister. Voortgangsrapportages worden gemaakt en of opgevraagd bij de uitbestedingspartij. Bij majeure IT-incidenten wordt er melding gemaakt bij de toezichthouders.

2.7. Incidentendossiers worden in een beveiligde omgeving bewaard zodat de vertrouwelijkheid wordt gewaarborgd. Indien er sprake is van de betrokkenheid van een Verbonden persoon worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen het dagelijks bestuur en de Compliance Officer toegang heeft tot deze gegevens.

2.8. 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.

2.9. Eenieder 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 3: Behandeling van Incidenten

3.1. Indien de directeur van het Pensioenfonds van mening is dat er sprake is van een Operationeel Incident of van een Beveiligingsincident brengt hij het Dagelijks Bestuur op de hoogte. Indien sprake is of kan zijn van een Integriteitsincident of een Overig Incident wordt het Dagelijks bestuur en de Compliance Officer op de hoogte gebracht. Indien het Incident de directeur van hetPensioenfonds betreft meldt de Compliance Officer dat aan het gehele bestuur. Door het Dagelijks bestuur wordt, na advies van de Compliance Officer, besloten of en wanneer andere organen van het Pensioenfonds, sleutelfunctiehouders en/of overige belanghebbenden op de hoogte worden gebracht van het Incident.

3.2. De afdeling van het Pensioenfonds waar zich het Operationele Incident of Beveiligingsincident heeft voorgedaan zorgt voor de afhandeling van het incident. De directeur van het Pensioenfonds coördineert de afhandeling van het incident met, afhankelijk van de aard van het incident, ondersteuning van de Compliance Officer.

3.3. De Compliance Officer behandelt de Integriteitsincidenten en Overige Incidenten, tenzij het bestuur, na advies van de Compliance Officer, besluit dat, gelet op de aard of achtergronden van het 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.

3.4. 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.

3.5. De Compliance Officer bewaakt de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties en rapporteert hierover aan het Bestuur. De Compliance Officer heeft de mogelijkheid om te escaleren naar de Raad van Toezicht.

3.6. Bij IT-incidenten wordt er door de uitbestedingspartij een melding gemaakt bij het bestuursbureau. Deze overlegt het incident met het dagelijks bestuur en deze classificeert het incident. Bij Majeure incidenten dienen binnen vier uur gemeld te worden bij de DNB en bij de AP binnen drie dagen.

3.7. De informatiemanager, directie en DB houden nauw contact met de uitbestedingspartij over de voortgang van het incident en ontvangen voortgangsrapportages.

3.8. Indien een incident als een datalek wordt geclassificeerd dan wordt de Procedure Meldplicht Datalekken.gevolgd.

Artikel 4: Afronding Incidenten

4.1. Na de behandeling van elk Incident wordt, ter afronding, door het Pensioenfonds 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 zullen 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 – voortvloeiend uit 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.

4.2. Bij majeure IT-incidenten wordt er een eindrapportage overlegd met het bestuur en de toezichthouder DNB. De eindrapportage wordt ook besproken in de risicomanagement commissie.

Artikel 5: Rapportage

5.1. 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 kan de Compliance Officer toezien op de daadwerkelijke opvolging.

5.2. In de rapportage(s) zoals die periodiek aan het bestuur worden aangeboden, wordt inzicht gegeven in het aantal en de classificatie van 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 de naar aanleiding van deze Incidenten genomen maatregelen.

5.3. De gevraagde rapportages door de toezichthouder bij majeure IT-incidenten worden door uitbestedingspartijen aangeleverd. De opvolging van de acties ligt bij het bestuursbureau en DB.

Artikel 6: Spoedeisend belang

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

6.2. De voorzitter van het bestuur is gehouden om de overige leden van het bestuur zo snel mogelijk op de hoogte te brengen van verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het bestuur voor te leggen.

Artikel 7: Melden Toezichthouder en overige communicatie

7.1. Door of namens het bestuur dan wel, indien noodzakelijk in verband met de voortgang, door de Compliance Officer 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 het pensioenfonds 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 pensioenfonds;
- mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het pensioenfonds;
- 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.

7.2. 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.

7.3. Het bestuur van het Pensioenfonds beslist over de communicatie, zowel intern als extern, met betrekking tot Incidenten.

Artikel 8: Omgang met meldingen

8.1 Het bestuur van het Pensioenfonds gaat er altijd vanuit dat een melding van een Incident te goeder trouw is gedaan, tot het moment dat zij overtuigd is geraakt van het tegendeel.

8.2 Het bestuur van het Pensioenfonds draagt er zorg voor dat een melder, ongeacht de wijze waarop deze melding heeft gemaakt van een Incident, op geen enkele wijze in zijn/haar/hen positie bij het pensioenfonds benadeeld wordt, voor zover te goeder trouw gehandeld is.

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

8.4 In geval van intrekking van een melding zal het bestuur van het Pensioenfonds, 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.

8.5 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: Overig

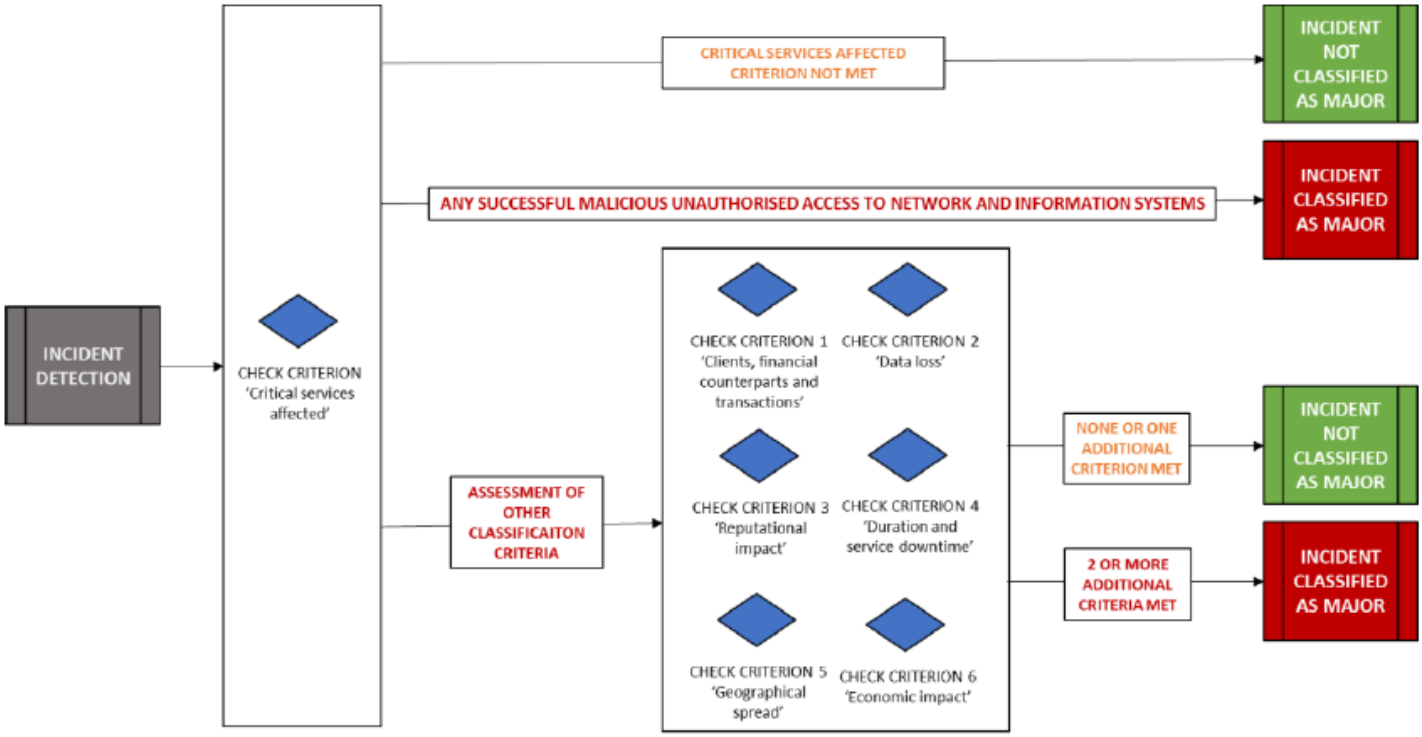
9.1. Deze regeling is vastgesteld door het bestuur van het pensioenfonds en in werking getreden op 18 september 2025

Bijlage A: DORA classificatie Incidenten

Het dagelijks bestuur zal bij een incident de volgende vragen beantwoorden om een (majeur) incident goed af te handelen:

- Wat is een incident (art. 3(8) DORA)?
- Hoe weet Mhpf dat er een incident heeft plaatsgevonden? (17(3) DORA)
- Wat zijn de gevolgen van het incident? Wat is de impact (art. 18 DORA)?
- Hoe wordt de impact beperkt? En zo snel mogelijk? (art. 17, lid 3, onder f) DORA)
- Hoe voorkomt Mhpf dat het incident zich herhaalt? (art. 13 lid 2 DORA)
- Hoe registreren we een incident en aan wie rapporteren we het incident (art. 17(1) DORA)?

Classificatie schema, criteria en materialiteitsdrempels voor ernstige ICT-incidenten



Voor het classificeren van ICT-incidenten moeten ondernemingen een aantal criteria hanteren die helpen bij het bepalen van de impact van het incident op de organisatie en externe stakeholders.

Deze criteria zijn:
• Het aantal en de relevantie van klanten die door het incident zijn getroffen. Hierbij gaat het om de klanten die gebruik maken van de diensten van de onderneming of de financiële tegenpartijen waar de onderneming een contractuele overeenkomst mee heeft. Daarnaast moeten ondernemingen vaststellen in hoeverre de impact van het incident dat de klant getroffen heeft, ook effect heeft op de doelstelling van de eigen onderneming. Tot slot wordt de relevantie van de klant bepaald door te kijken naar het effect van de klant op het vermogen van de instelling om haar doelstellingen te behalen;

• Het verlies van gegevens als gevolg van het incident. Hiervoor moeten ondernemingen bepalen of gegevens nog toegankelijk zijn (beschikbaarheid), of de gegevens onjuist of onvolledig zijn (integriteit) en of de gegevens zijn benaderd of openbaar zijn gemaakt door ongeautoriseerde gebruikers (vertrouwelijkheid);

• De mate waarin de getroffen diensten als cruciaal voor de onderneming kunnen worden aangemerkt.

Dit is het geval wanneer het incident invloed heeft gehad op ICT-diensten die belangrijke of kritieke bedrijfsfuncties ondersteunen;

• De reputatieschade die het incident heeft veroorzaakt. Om de reputatieschade vast te stellen, kijken ondernemingen hoeveel aandacht het incident heeft gekregen in de markt. Hierbij kan onder andere worden onderzocht of het incident in de media is gekomen, of er klachten zijn binnengekomen vanuit klanten of dat de onderneming als gevolg van het incident niet kan voldoen aan wettelijke eisen;

• De duur van het incident. Om dit te bepalen meet de onderneming de tijd tussen het moment dat het incident plaatsvindt en het moment dat het incident is opgelost. Wanneer het startmoment niet kan worden vastgesteld, kan de onderneming het moment gebruiken wanneer het is vastgesteld of wanneer het is vastgelegd in logbestanden of andere databronnen. Als de precieze oplostijd niet bekend is, mogen instellingen een schatting maken om het einde van het incident te bepalen;

• De geografische spreiding van de gebieden die door het incident zijn getroffen. Om de geografische spreiding te bepalen, beoordelen instellingen onder andere de impact van het incident op de klanten, andere kantoren of instellingen binnen de groep in tenminste twee EU-lidstaten;

• De economische effecten van het incident in absolute en relatieve termen. Hierbij gaat het om directe en indirecte kosten en verliezen als gevolg van het incident

	Aanvullende classificatie criteria			
	Gegevensverlies	**Reputatieschade**	**Duur serviceonderbreking.**	**Economische impact**
Materialiteitsdrempel	A. Elke impact op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens, die een negatieve impact heeft of zal hebben op de implementatie van de bedrijfsdoelstellingen van Het pensioenfonds of op het voldoen aan regelgevende vereisten. B. Elk kwaadaardige en ongeautoriseerde toegang vindt plaats tot netwerk- en informatiesystemen die niet onder item 'A.' vallen, wat kan leiden tot gegevensverlies.	Alle reputatie-impact beschreven in de criteria aangegeven hieronder.	A. De duur van het incident is langer dan 24 uur; of B. b) De onderbreking van de dienst is langer dan 2 uur voor ICT-diensten die kritieke of belangrijke diensten ondersteunen.	Kosten en verliezen geleden door Het pensioenfonds overschrijden of zullen waarschijnlijk € 100.000, overschrijden (kan gebaseerd zijn op schattingen waar werkelijke waarden niet kunnen worden bepaald).
Criteria	1. Beschikbaarheid: de gegevens zijn tijdelijk of permanent ontoegankelijk of onbruikbaar gemaakt; 2. Authenticiteit: er is sprake van aangetaste betrouwbaarheid van de bron van gegevens; 3. Integriteit: de gegevens zijn onnauwkeurig of onvolledig door niet-geautoriseerde wijzigingen 4. Vertrouwelijkheid: de gegevens worden toegankelijk gemaakt voor of bekendgemaakt aan een onbevoegde partij	De reputatie-impact wordt aangetoond door een van de onderstaande situaties: A. Het incident is zichtbaar in de media; of B. Het pensioenfonds heeft herhaalde klachten ontvangen van deelnemers, werkgevers of andere partijen over de betrokken kritieke diensten; of	1. De duur wordt gemeten vanaf het moment dat een incident optreedt of wordt gedetecteerd, tot het moment dat het is opgelost (schatting als het nog niet bekend is). 2. De onderbreking van de dienst wordt gemeten vanaf het moment dat de service volledig/gedeeltelijk niet beschikbaar/vertraagd is	Soorten directe en indirecte gemaakte kosten: A. Verloren fondsen of financiële activa aansprakelijkheid, inclusief diefstal; B. Vervangings- of verplaatsingskosten; C. Personeelskosten; D. Kosten voor niet-naleving van het contract;

of systeem.	C. Het pensioenfonds is (waarschijnlijk) niet in staat om te voldoen aan wet- en regelgeving; of D. Het pensioenfonds waarschijnlijk deelnemers of werkgevers verliest wat materiële impact heeft op de bedrijfsvoering van Het pensioenfonds. De mate van zichtbaarheid van het incident moet in aanmerking worden genomen.	voor deelnemers, werkgevers of andere interne of externe gebruikers, tot de activiteiten zijn hersteld naar hetzelfde niveau als voor het incident.	E. Kosten voor klanttevredenhei en compensatie; F. Gederfde inkomsten; G. Communicatiekosten; H. Advieskosten (gebaseerd op beschikbare gegevens op het moment van rapportage).

Deze stappen samen zorgen voor een adequaat proces om een ICT-incident te classificeren af te handelen. Dan volgt er nog de meldplicht aan de bevoegde autoriteiten, zoals een AFM of DNB, zoals geregeld in artikel 19 DORA.

1. Nadat het dagelijks bestuur heeft vastgesteld dat een majeur IT-incident zich heeft voorgedaan en de relevante feiten helder zijn, zal DNB door of namens het bestuur als volgt geïnformeerd worden.
   a. Eerste kennisgeving: binnen vier (4) uur vanaf de classificatie van het ICT-incident als ernstig, maar niet later dan 24 uur vanaf het moment van detectie van het Ernstige ICT-incident, wordt er een eerste kennisgeving toegestuurd;
   b. Tussentijds verslag: binnen 72 uur vanaf de classificatie van het ICT-incident als ernstig, of zodra de reguliere activiteiten zijn hersteld en het Pensioenfonds functioneert als voorheen het ernstige ICT-incident;
   c. Eindverslag: uiterlijk een maand na de classificatie van het ICT-incident als ernstig, tenzij het incident nog niet is opgelost. In dat laatste geval wordt het eindrapport de dag na de definitieve oplossing van het ernstige ICT-incident worden ingediend.

2. Indien het Pensioenfonds niet in staat is om de gestelde tijdslimieten te halen, wordt DNB hiervan zonder onnodige vertraging op de hoogte gesteld, uiterlijk binnen 24 uur na het constateren van de vertraging. Tevens licht het Pensioenfonds de specifieke redenen voor deze vertraging toe aan DNB.

3. Bij het indienen van een tussentijds of eindrapport zal het Pensioenfonds, indien van toepassing, de informatie die eerder werd verstrekt bijwerken.

4. Indien het Pensioenfonds na een evaluatie van het ernstig ICT-incident tot de conclusie komt dat het incident op geen enkel moment voldeed aan de classificatiecriteria en materialiteitsdrempels van een ernstig ICT-incident, zal het Pensioenfonds een eindverslag indienen waarin uitsluitend de informatie met betrekking tot de herclassificatie van het ernstige ICT-incident naar een niet-ernstig ICT-incident wordt opgenomen.

5. In elk afzonderlijk geval zal worden onderzocht of het Pensioenfonds of de uitbestedingspartij de melding aan DNB zal doen.

6. In het geval dat het Pensioenfonds een derde partij inschakelt om meldingen en rapporten bij DNB in te dienen, zal het Pensioenfonds DNB voorafgaand aan de eerste melding of rapportage op de hoogte stellen van deze uitbestedingsregeling. het Pensioenfonds zal DNB voorzien van de naam en contactgegevens van de derde partij die de melding namens het Pensioenfonds zal indienen. Bovendien

zal het Pensioenfonds DNB informeren indien dergelijke uitbesteding niet langer van toepassing is of wordt beëindigd.

7. Op verzoek van DNB verstrekt het Pensioenfonds een verslag betreffende de schatting van de totale (jaarlijkse) kosten en verliezen die voortvloeien uit ernstige ICT-gerelateerde incidenten.