Formulier ten behoeve van meldingen van incidenten door aanbieders essentiële diensten

Als bedoeld in art.10 lid 2 en lid 3 van de Wet beveiliging netwerk- en informatiesystemen
Graag zo volledig mogelijk invullen. Onverwijld melden na ontdekking. Uw ingevuld formulier beveiligd sturen naar wbni@agentschaptelecom.nl

0. De volgende velden zijn verplicht in te vullen bij een nieuwe melding

0.1 Algemene gegevens melding

Verplicht in te vullen velden bij een nieuwe melding

Datum en tijd melding incident	
Nieuwe / Vervolg melding	☐ Nieuwe melding ☐ Aanvullen of wijzigen bestaande melding ☐ Eind melding
Status incident	☐ Incident staat nog open ☐ Incident is gesloten ☐ Ingetrokken
Hoe schat u de kans in dat dit incident tot aanzienlijke gevolgen zal leiden? Vul dit veld in als het een incident betreft dat nog geen aanzienlijke gevolgen heeft	☐ Hoog ☐ Midden ☐ Laag
Hoe schat u de impact van de schade in als de aanzienlijke gevolgen zijn bereikt? Vul dit veld in als het een incident betreft dat nog geen aanzienlijke gevolgen heeft	☐ Hoog ☐ Midden ☐ Laag

0.2 Gegevens meldende partij

Verplicht in te vullen velden bij een nieuwe melding

Bedrijfsnaam		
Wat voor soort essentiële dienstverlener bent u?	☐ Elektriciteit ☐ Gas ☐ Olie ☐ TLD (Top Level Domain) ☐ DNS (Domain Name Service) ☐ IX (Internet eXchange)	
Melder	Naam	
	Functie	
	E-mailadres	
	Telefoonnummer	

	Beschikbaarheid	
Contactpersoon Vul dit veld in als deze persoon een andere is dan de melder	Naam	
	Functie	
	E-mailadres	
	Telefoonnummer	

0.3 Gegevens over het incident

Verplicht in te vullen velden bij een nieuwe melding, hiermee voldoet men aan de meldplicht onder de wet

Incident bij Digitaledienstverlener met gevolgen voor de continuïteit van uw essentiële dienst	☐ Ja, naam digitaledienstverlener ☐ Nee
Aard en omvang incident	
Datum en tijd vermoedelijke aanvang incident	
Mogelijke gevolgen incident in en buiten Nederland	
Prognose benodigde hersteltijd	
Beschrijving, zo mogelijk, maatregelen die genomen zijn om gevolgen te beperken	
Beschrijving, zo mogelijk, maatregelen die genomen zijn om gevolgen te voorkomen	

1. De volgende velden kunnen later, na een initiële melding, aangevuld worden

1.1 Beschrijving incident vanuit een ICT perspectief

Deze velden kunnen later na een initiële melding aangevuld worden

Categorie incident meer dan één antwoord mogelijk	☐ Beschikbaarheid ☐ Integriteit ☐ Vertrouwelijkheid ☐ Authenticiteit		
Geraakte onderdelen van de essentiële dienst in uw organisatie meer dan één antwoord mogelijk	☐ Software ☐ Hardware ☐ Systeem ☐ Gegevens ☐ Personen		
	Toelichting		
Waardoor is het incident opgetreden meer dan één antwoord mogelijk	**Systeem falen** ☐ Software fouten en bugs ☐ Hardware falen en bugs ☐ Fouten in procedure ☐ Overig **Natuurrampen** ☐ Storm ☐ Aardbeving ☐ Overig	**Menselijke factor** ☐ Moedwillig nalatig gebruik of beheer ☐ Niet-moedwillig nalatig gebruik of beheer **Malafide acties** ☐ Cyber aanval ☐ Vandalisme ☐ Diefstal ☐ Overig	**3e partij** ☐ Leverancier ☐ Subcontractant
	Toelichting		
Omschrijving hoe ontdekt			
Datum en tijd ontdekking incident			
Vermoedelijke manier van aanvallen Vul dit veld in als hierboven bij malafide acties een vink is gezet. Meer dan één antwoord mogelijk	☐ **Misbruik van kwetsbaarheden**	☐ **Malware**	☐ **Gerichte aanval**
	Toelichting	Toelichting (bijv. IoCs)	Toelichting (bijv. IoCs)
	☐ **Denial of service**	☐ **Ongeautoriseerde**	☐ **Overig**

		toegang	
	Toelichting (bijv. IoCs)	Toelichting	Toelichting

1.2 Geraakte gegevens

Deze velden kunnen later na een initiële melding aangevuld worden

Geraakte gegevens meer dan één antwoord mogelijk	**Persoonsgegevens** ☐ Ja. Geef hieronder aan welke persoonsgegevens zijn geraakt. Benoem hierbij de bijzondere persoonsgegevens.	
	Toelichting	
	Overige gegevens ☐ Ja. Geef hieronder aan welke gegevens zijn geraakt. ☐ N.v.t.	
	Toelichting	

1.3 Melding aan andere instanties

Deze velden kunnen later na een initiële melding aangevuld worden

Welke andere instanties heeft u op de hoogte gebracht van dit incident?	
Mag Agentschap Telecom uw meldgegevens delen met NCSC (de CSIRT voor de AEDs)?	☐ Ja ☐ Nee
Mag Agentschap Telecom uw meldgegevens delen met Autoriteit Persoonsgegevens? Alleen als er persoonsgegevens geraakt zijn	☐ Ja ☐ Nee
Mag Agentschap Telecom uw meldgegevens delen met andere toezichthouders?	☐ Ja ☐ Nee
Heeft u aangifte gedaan bij de politie? Vul dit veld in als hierboven bij malafide acties een vink is gezet	☐ Ja ☐ Nee

1.4 Onderzoek en restrisico

Deze velden kunnen later na een initiële melding aangevuld worden

Onderzoek naar incident	Prognose duur onderzoek	
	Ondersteuning door derden	
Restrisico acceptatie		

1.5 Overig

Deze velden kunnen later na een initiële melding aangevuld worden

Inschatting impact op andere geraakte deelsectoren meer dan één antwoord mogelijk	**Digitale dienstverlener** ☐ Online marktplaats ☐ Online zoekmachine ☐ Cloud computerdienst **Welke dienst is geraakt?**	**Vervoer** ☐ Luchtvervoer ☐ Spoorvervoer ☐ Vervoer en water ☐ Vervoer over de weg **Welke essentiële dienst is geraakt?**	**Gezondheidszorg** ☐ Zorginstellingen (wo ziekenhuizen, privé klinieken) **Welke essentiële dienst is geraakt?**
	Energie ☐ Elektriciteit ☐ Aardolie ☐ Gas **Welke essentiële dienst is geraakt?**	**Bankwezen** ☐ Banken **Welke essentiële dienst is geraakt?**	**Levering en distributie drinkwater** ☐ Leverancier ☐ Distributeur **Welke essentiële dienst is geraakt?**

	Vitaal/niet essentieel ☐ Nucleair ☐ Telecom ☐ Vertrouwensdiensten ☐ Rijksoverheid ☐ Waterkeren/-beheren **Welke dienst is geraakt?**	**Infrastructuur voor de financiële markt** ☐ Exploitant handelsplatform ☐ Centrale tegenpartij **Welke essentiële dienst is geraakt?**	**Digitale infrastructuur** ☐ Internetknoop-punten ☐ DNS leveranciers ☐ Register voor top-leveldomeinnamen **Welke essentiële dienst is geraakt?** **Momenteel nog onbekend** ☐ Nog onbekend
Afsluiting incident	Datum en tijd		
	Reden		

Opsturen meldformulier
Graag zo volledig mogelijk invullen. Onverwijld melden na ontdekking. Uw ingevuld formulier beveiligd sturen naar wbni@agentschaptelecom.nl

Toelichting op het formulier ten behoeve van meldingen van incidenten door aanbieders essentiële diensten

Een cybersecurity incident met aanzienlijke gevolgen voor de verlening van uw essentiële dienst dient op grond van de Wet beveiliging netwerk- en informatiesystemen onverwijld gemeld te worden bij Agentschap Telecom.

Naast de verplichte velden, wordt u verzocht om dit formulier zo compleet mogelijk in te vullen. Door deze verplichte velden (blok 0) door te geven op het moment van een melding, voldoet u aan de meldplicht uit de wet. De andere gegevens (blok 1) heeft Agentschap Telecom nodig om haar onderzoek te kunnen uitvoeren. De mogelijkheid bestaat om een melding later aan te vullen zodra er meer informatie beschikbaar is. Als de gevoeligheid van de informatie dit vereist, dient u de melding op een beveiligde wijze te verzenden.

Een cybersecurity incident is elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van de netwerk- en informatiesystemen. Onder de beveiliging van netwerk- en informatiesystemen wordt verstaan de mate van betrouwbaarheid om bestand te zijn tegen acties die beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit schaden. Het gaat hier om de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn.

0.1 Algemene gegevens melding

Verplicht in te vullen velden bij een nieuwe melding

Datum en tijd melding incident	Vul hier de datum en tijd in van deze melding. Gebruik de volgende datum/tijd indeling bij het invullen van dit veld dd/mm/jjjj uu:mm (d = dag, m = maand, j = jaar, u = uur, m = minuut).
Nieuwe / Vervolg melding	Geef aan of deze melding een nieuwe, vervolg of eind melding betreft. Een initiële melding (een nieuwe melding) betreft een melding van een incident dat niet eerder bij Agentschap Telecom is gemeld. Van een vervolgmelding is sprake als u informatie over een eerder gemeld incident aanvult. Maak één keuze uit de aangeboden opties.
Status incident	Geef aan of de oorzaak inmiddels is bepaald en of het incident nog in onderzoek is. Geef hier ook aan als u een incidentmelding wilt intrekken. Maak één keuze uit de aangeboden opties.
Hoe schat u de kans in dat dit incident tot aanzienlijke gevolgen zal leiden?	Vul dit veld in als het een incident betreft dat nog *geen* aanzienlijke gevolgen heeft.
Hoe schat u de schade in als de aanzienlijke gevolgen zijn bereikt?	Vul dit veld in als het een incident betreft dat nog *geen* aanzienlijke gevolgen heeft.

0.2 Contactgegevens meldende partij

Verplicht in te vullen velden bij een nieuwe melding

Bedrijfsnaam	De naam van de aangewezen aanbieder van essentiële diensten (AED). Gebruik vrije tekst om dit veld in te vullen.
Wat voor soort essentiële dienstverlener bent u?	Vermeld ook hier de soort essentiële dienst die u aanbiedt. Mogelijke diensten zijn elektriciteit, gas, olie. Of binnen de digitale infrastructuur TDL, DNS of IX. Maak één of meer keuzes uit de aangeboden opties.
Melder	Gegevens van de persoon die meldt. Gebruik vrije tekst om deze velden in te vullen.
Contactpersoon	Gegevens van de contactpersoon. Dit kan een andere persoon zijn dan degene die een melding doorgeeft. Gebruik vrije tekst om dit veld in te vullen.

0.3 Gegevens over het incident

Verplicht in te vullen velden bij een nieuwe melding, hiermee voldoet men aan de meldplicht onder de wet

Incident bij Digitaledienstverlener met	Een AED meldt ook incidenten die aanzienlijke gevolgen hebben voor hun essentiële diensten maar die veroorzaakt zijn door incidenten die zich hebben voorgedaan bij een

gevolgen voor de continuïteit van uw essentiële dienst	DSP waar ze diensten van afnemen. Conform art. 10.3.
Aard en omvang incident	Geef een omschrijving van het incident. Denk hierbij aan het beantwoorden van vragen zoals: welke dienst is geraakt en hoe, waar in de organisatie manifesteert het incident zich, hoe is het zichtbaar geworden dat er sprake is van een incident, welke zichtbare gevolgen zijn er, etc. Conform art. 11a. Gebruik vrije tekst om dit veld in te vullen.
Datum en tijd vermoedelijke aanvang incident	Vul hier de vermoedelijke datum en tijd in van de aanvang van het incident. Conform art. 11b. Gebruik de volgende datum/tijd indeling bij het invullen van dit veld dd/mm/jjjj uu:mm (d = dag, m = maand, j = jaar, u = uur, m = minuut).
Mogelijke gevolgen incident in en buiten Nederland	Geef hier aan op welke manier andere partijen binnen de EU last hebben van dit incident. Probeer hierbij de gevolgen van het incident te kwantificeren in termen van het vermogen aan elektriciteit, gas of olie dat binnen een bepaalde periode verloren is gegaan. Conform art. 11c. Gebruik vrije tekst om dit veld in te vullen.
Prognose benodigde hersteltijd	Geef een inschatting hoeveel tijd u nog (na melding) nodig heeft om het incident af te kunnen sluiten. Conform art. 11d. Gebruik vrije tekst om dit veld in te vullen.
Beschrijving, zo mogelijk, maatregelen die genomen zijn om gevolgen te beperken	Beschrijf de maatregelen die zijn getroffen of die u gaat treffen om de gevolgen van het incident zoveel mogelijk in te perken. Dit kunnen tijdelijke maatregelen zijn. Conform art. 11e. Gebruik vrije tekst om dit veld in te vullen.
Beschrijving, zo mogelijk, maatregelen die genomen zijn om gevolgen te voorkomen	Onder voorgenomen maatregelen verstaan we die activiteiten die u heeft genomen of gepland om het incident en de gevolgen hiervan structureel in te perken en om herhaling van het incident te voorkomen. Conform art. 11e. Gebruik vrije tekst om dit veld in te vullen.

1.1 Beschrijving incident vanuit een ICT perspectief

Deze velden kunnen later in een vervolg melding aangevuld worden

Categorie incident	Een beveiligingsincident kan één of meer van de volgende aspecten raken: – Beschikbaarheid: de mate waarin de dienst of de informatie hierin in bedrijf of benaderbaar is op het moment dat dit vereist is, – Integriteit: de mate waarin de dienst of informatie hierin ongeautoriseerd (moedwillig of onbedoeld) is aangepast, – Vertrouwelijkheid: de waarborg dat de dienst of de informatie hierin alleen door een gedefinieerde groep van geautoriseerde gebruikers toegankelijk is, – Authenticiteit: de mate waarin de partijen kunnen aantonen dat zij betrokken zijn bij een transactie. Maak één of meer keuzes uit de aangeboden opties.
Geraakte onderdelen van de essentiële dienst in uw organisatie	Geef aan welk deel van uw dienst is geraakt door het incident. Probeer hierbij aan te geven welk ICT onderdeel van de dienst geraakt is. Het is mogelijk dat meerdere ICT onderdelen zijn geraakt binnen dezelfde dienst. Maak één of meer keuzes uit de aangeboden opties.
Waardoor is het incident opgetreden	Geef aan waardoor het incident is veroorzaakt, voor zover dit bekend is. Meerdere antwoorden zijn mogelijk. Licht de gemaakte keuze(s) toe. Maak één of meer keuzes uit de aangeboden opties.
Omschrijving hoe ontdekt	Schets kort hoe het incident is ontdekt. Denk hier aan mogelijkheden zoals uitval van systeem, tijdens systeem onderhoud, tijdens monitoring systemen, evaluatie logbestanden, audit resultaten, etc. Gebruik vrije tekst om dit veld in te vullen.
Datum en tijd ontdekking incident	Vul hier de datum en tijd van de ontdekking van het incident in. Gebruik de volgende datum/tijd indeling bij het invullen van dit veld dd/mm/jjjj uu:mm (d = dag, m = maand, j = jaar, u = uur, m = minuut).

Vermoedelijke manier van aanvallen	Geef hier aan hoe de aanval, die het incident heeft veroorzaakt, is gepleegd. Meerdere antwoorden zijn mogelijk. Licht dit toe waar mogelijk. Geef in de toelichting ook aan als er indicators of compromise (IoCs) zijn ontdekt. IoCs zijn indicatoren dat een systeem of proces is gecompromitteerd, bijv. hash waarden, protocollen, IP poorten, etc. U hoeft de gevonden indicatoren niet exact te benoemen. Vul dit veld in als hierboven bij malafide acties een vink is gezet, dus als er sprake is van een aanval. Maak één of meer keuzes uit de aangeboden opties.

1.2 Geraakte gegevens

Deze velden kunnen later in een vervolg melding aangevuld worden

Geraakte gegevens	Geef een inschatting welke gegevens geraakt zijn bij dit incident. Vermeld de persoonsgegevens en de bijzondere persoonsgegevens expliciet.

1.3 Melding aan andere instanties

Deze velden kunnen later in een vervolg melding aangevuld worden

Welke andere instanties heeft u op de hoogte gebracht van dit incident?	Geef aan welke andere instanties u op de hoogte heeft gebracht van dit incident. Geef ook aan hoe en wanneer u dat heeft gedaan. Denk hierbij aan instanties zoals NCSC (CSIRT), Autoriteit Persoonsgegevens. Gebruik vrije tekst om dit veld in te vullen.
Mag Agentschap Telecom uw meldgegevens delen met NCSC (de CSIRT voor de AEDs)?	Hiermee kunt u AT toestemming geven om deze meldgegevens te delen met NCSC (CSIRT). Maak één keuze uit de aangeboden opties.
Mag Agentschap Telecom uw meldgegevens delen met Autoriteit Persoonsgegevens?	Hiermee kunt u AT toestemming geven om deze meldgegevens te delen met Autoriteit Persoonsgegevens. Dit hoeft uiteraard alleen als er persoonsgegevens geraakt zijn. Maak één keuze uit de aangeboden opties.
Mag Agentschap Telecom uw meldgegevens delen met andere toezichthouders?	Hiermee kunt u AT toestemming geven om deze meldgegevens te delen met andere toezichthouders. Maak één keuze uit de aangeboden opties.
Heeft u aangifte gedaan bij de politie?	Als er sprake is van een malafide actie, een aanval, geeft u hier aan of er aangifte is gedaan bij de politie. Maak één keuze uit de aangeboden opties.

1.4 Onderzoek en restrisico

Deze velden kunnen later in een vervolg melding aangevuld worden

Onderzoek naar incident	Prognose duur onderzoek	Maak een inschatting hoeveel tijd u nog (na melding) nodig heeft voor onderzoek naar het incident. Gebruik vrije tekst om dit veld in te vullen.
	Ondersteuning door derden	Als voor het oplossen van het incident gebruik is/wordt gemaakt van diensten van derden, geeft u dan aan welke partijen u hiervoor heeft ingezet en waarvoor. Gebruik vrije tekst om dit veld in te vullen.
Restrisico acceptatie	Geef aan welke risico's niet door maatregelen worden afgedekt en hoe u met deze restrisico's om zal gaan. Gebruik vrije tekst om dit veld in te vullen.	

1.5 Overig

Deze velden kunnen later in een vervolg melding aangevuld worden

Inschatting impact op andere geraakte deelsectoren	Geef een inschatting van de impact van het gemelde incident op andere deelsectoren die in de Wet beveiliging netwerk- en informatiesystemen worden genoemd. Het is van belang dat het incident beperkt blijft. Als een incident wijder verspreid is dan binnen één

	omgeving of dienst dan is het van belang dat u dit hier aangeeft. Geef bij 'geraakte vitale dienst' aan welke vitale dienst in de andere deelsector geraakt is. Maak één of meer keuzes uit de aangeboden opties. Licht waar mogelijk de gemaakte keuze in vrije tekst bij toelichting.
Afsluiting incident	Als het incident is ingetrokken of afgehandeld, vult u dan de reden en datum in. Gebruik de volgende datum/tijd indeling bij het invullen van dit veld dd/mm/jjjj uu:mm (d = dag, m = maand, j = jaar, u = uur, m = minuut).

Opsturen meldformulier
Graag zo volledig mogelijk invullen. Onverwijld melden na ontdekking. Uw ingevuld formulier beveiligd sturen naar **wbni@agentschaptelecom.nl**