Procedure meldplicht significante incidenten

CBW-P01

Stichting Voorbeeldzorg

Hoe wij bepalen of een incident significant is en hoe wij binnen 24 uur, 72 uur en één maand melden aan het CSIRT en de toezichthouder en onze afnemers informeren.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de Cyberbeveiligingswet Toolkit · alle 50 documenten: www.maasiso.nl/toolkits/cyberbeveiligingswet/

Documentinformatie

DOCUMENTTITEL	Procedure meldplicht significante incidenten
DOCUMENTNUMMER	CBW-P01
VERSIE	1.0
DATUM	19 oktober 2026
AUTEUR	Sanne de Vries
GOEDGEKEURD DOOR	Sanne de Vries
ORGANISATIE	Stichting Voorbeeldzorg
CLASSIFICATIE	Intern

Versiehistorie

Versie	Datum	Auteur	Wijzigingen
1.0	19 oktober 2026	Sanne de Vries	Initiële versie

ART. 25 CBW · ART. 26 CBW · ART. 24 CBB · ART. 27 CBW · ART. 28 CBW · ART. 29 CBW · ART. 30 CBW

1. Doel

Een significant incident melden wij aan ons CSIRT en onze toezichthouder, binnen vaste termijnen. Deze procedure zorgt dat wij op tijd beslissen, op tijd melden en kunnen laten zien waarom wij een incident wel of niet hebben gemeld. De afhandeling van het incident zelf staat in ISB-P03 Incidenten melden en afhandelen.

2. Termijnen in één oogopslag

De klok begint te lopen op het moment dat wij van het significante incident weten. Wij melden zo snel als het kan; de termijnen zijn uiterste grenzen.

Stap	Uiterlijk	Wat wij aanleveren	Artikel
Vroegtijdige waarschuwing	Binnen 24 uur	Dat er een significant incident is, met de eerste gegevens	Cbw 26
Melding	Binnen 72 uur	Bijgewerkt beeld en eerste beoordeling van ernst en gevolgen	Cbw 27
Tussentijds verslag	Op verzoek	De stand van zaken	Cbw 28
Eindverslag	Binnen één maand na de melding	Volledige beschrijving, oorzaak en maatregelen	Cbw 29
Afnemers informeren	Direct, als hun dienst geraakt kan worden	Wat er speelt en wat zij kunnen doen	Cbw 30

3. Rollen

Rol	Taak
ISMS-coördinator	Beoordeelt of het incident significant is, stelt de meldingen op en bewaakt de termijnen.
Directie	Besluit over de melding als de beoordeling niet eenduidig is en keurt het eindverslag goed.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de Cyberbeveiligingswet Toolkit · alle 50 documenten: www.maasiso.nl/toolkits/cyberbeveiligingswet/

Rol	Taak
IT-beheerder	Levert de technische feiten: wat is geraakt, sinds wanneer, wat is gedaan.
Privacyverantwoordelijke	Beoordeelt of er ook een datalek is dat aan de Autoriteit Persoonsgegevens moet worden gemeld.
Meldfunctionaris	Sanne de Vries, 06 12 34 56 78. Contactpersoon voor het CSIRT en de toezichthouder.
Vervanger meldfunctionaris	Tim Hendriks, 06 23 45 67 89

De meldfunctionaris en de vervanger zijn ook buiten kantoortijd bereikbaar. Zij hebben de inloggegevens voor het meldpunt en kunnen daar ook bij als onze eigen systemen uitvallen.

4. Is het incident significant?

De ISMS-coördinator beoordeelt dit voor elk incident met niveau hoog, en bij twijfel ook voor niveau midden. De beoordeling gebeurt uiterlijk vier uur na de melding van het incident.

Een incident is significant als ten minste één van deze vragen met ja wordt beantwoord:

Vraag	Voorbeelden
Veroorzaakt het incident een ernstige verstoring van onze diensten, of kan het dat doen?	Een kernsysteem ligt uren stil; afnemers kunnen de dienst niet gebruiken.
Veroorzaakt het incident financieel verlies voor onze organisatie, of kan het dat doen?	Herstelkosten, omzetverlies of losgeld van betekenis.
Treft het incident anderen met aanzienlijke materiële of immateriële schade, of kan het dat doen?	Gegevens van afnemers zijn gestolen; een aanval verspreidt zich via onze systemen naar klanten.

Onze eigen drempels:

Onderwerp	Drempel waarboven wij het incident als significant behandelen
Uitval van een kerndienst	Langer dan vier uur, of langer dan één uur voor het patiëntendossier
Aantal geraakte afnemers of gebruikers	Meer dan 500 patiënten of één hele locatie
Financiële schade	Verwachte schade boven 100.000 euro
Vertrouwelijke gegevens	Elke diefstal van medische of andere vertrouwelijke gegevens door een aanvaller

Bij twijfel melden wij. Een waarschuwing te veel is beter dan een melding te laat.

Is het incident niet significant, dan noteert de ISMS-coördinator de reden in het incidentrapport (T-ISB-001 Incidentrapport).

5. Melden

Alle meldingen doen wij via het meldpunt dat de overheid daarvoor heeft ingericht: het meldportaal van de overheid, met het organisatieaccount; inloggegevens in de noodenvelop. Via dat meldpunt bereikt de melding het CSIRT en de toezichthouder. Elke melding leggen wij vast in T-CBW-001 Meldingsdossier significant incident.

5.1 Vroegtijdige waarschuwing (binnen 24 uur)

In de waarschuwing staat:

- of het incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt;

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de Cyberbeveiligingswet Toolkit · alle 50 documenten: www.maasiso.nl/toolkits/cyberbeveiligingswet/

- of het incident gevolgen in andere landen kan hebben;
- de contactgegevens van de meldfunctionaris;
- het vermoedelijke tijdstip waarop het incident begon;
- zo mogelijk: de aard van het incident en de gevolgen die op dat moment merkbaar zijn;
- zo mogelijk: de verwachte hersteltijd;
- zo mogelijk: de maatregelen die wij hebben genomen of gaan nemen.

Wij wachten niet tot alles bekend is. Wat wij nog niet weten, melden wij als onbekend.

5.2 Melding (binnen 72 uur)

In de melding staat:

- een update van de gegevens uit de waarschuwing;
- een eerste beoordeling van het incident, met de ernst en de gevolgen;
- als die beschikbaar zijn: de technische kenmerken waaraan de aanval te herkennen is, zoals IP-adressen, bestandsnamen of domeinen;
- alle beschikbare informatie over mogelijke gevolgen in andere landen.

5.3 Tussentijds verslag (op verzoek)

Vraagt het CSIRT of de toezichthouder om een tussentijds verslag, dan levert de meldfunctionaris dat binnen de gevraagde termijn.

5.4 Eindverslag (binnen één maand na de melding)

In het eindverslag staat:

- een gedetailleerde beschrijving van het incident, de ernst en de gevolgen;
- het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;
- de maatregelen die zijn genomen en die nog lopen;
- als dat speelt: de gevolgen in andere landen.

Duurt het incident na een maand nog voort, dan dienen wij op dat moment een voortgangsverslag in met dezelfde onderwerpen. Het eindverslag volgt binnen één maand nadat het incident is afgehandeld.

De directie keurt het eindverslag goed voordat het wordt ingediend.

6. Afnemers informeren

Kan het incident de dienstverlening aan onze afnemers raken, dan informeren wij hen direct. Wij vertellen wat er speelt, wat het voor hen betekent en wat zij zelf kunnen doen.

Is er een significante dreiging die onze afnemers kan raken, dan laten wij hen direct weten welke maatregelen zij kunnen nemen. Als dat nodig is, vertellen wij ook wat de dreiging is.

Gegeven	Invullen
Wie stelt het bericht op	Afdeling communicatie, met de ISMS-coördinator
Wie keurt het bericht goed	Voorzitter raad van bestuur
Kanalen	E-mail aan contactpersonen, bericht op de website, telefonisch voor de grootste afnemers
Waar de contactlijst staat	Crisismap, ook op papier

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de Cyberbeveiligingswet Toolkit · alle 50 documenten: www.maasiso.nl/toolkits/cyberbeveiligingswet/

7. Andere meldingen

Eén incident kan tot meer meldingen leiden. De termijnen lopen naast elkaar.

Melding	Wanneer	Waar geregeld
Datalek aan de Autoriteit Persoonsgegevens	Als persoonsgegevens zijn geraakt, binnen 72 uur	ISB-P03 Incidenten melden en afhandelen
Melding aan klanten op grond van een contract	Volgens de afspraak in het contract	ISB-P03 Incidenten melden en afhandelen
Aangifte bij de politie	Bij een strafbaar feit, na besluit van de directie	ISB-P03 Incidenten melden en afhandelen
Melding aan de verzekeraar	Volgens de polis	Cyberverzekering; melden via de schadelijn

Incidenten die niet significant zijn, bijna-incidenten en dreigingen mogen wij vrijwillig melden. De ISMS-coördinator besluit daarover.

8. Oefenen en evalueren

- Wij oefenen de meldprocedure elk jaar, samen met de crisisoefening: van de eerste beoordeling tot en met het invullen van de waarschuwing.
- Na elk significant incident evalueren wij binnen vier weken na het eindverslag of de termijnen zijn gehaald en wat beter kan.

9. Registraties

Registratie	Waar	Bewaartermijn
Meldingsdossiers	SharePoint, map ISMS/Meldingen	drie jaar, tenzij een wet of contract een langere termijn voorschrijft
Beoordelingen van incidenten die niet zijn gemeld	In het incidentrapport	drie jaar, tenzij een wet of contract een langere termijn voorschrijft
Berichten aan afnemers	SharePoint, map ISMS/Meldingen	drie jaar, tenzij een wet of contract een langere termijn voorschrijft
Verslagen van oefeningen	SharePoint, map ISMS/Continuïteit	drie jaar, tenzij een wet of contract een langere termijn voorschrijft

10. Verwante documenten

Document	Titel
ISB-P03	Incidenten melden en afhandelen
T-CBW-001	Meldingsdossier significant incident
T-ISB-001	Incidentrapport
ISB-P04	Bedrijfscontinuïteit
CBW-001	Toepasselijkheid en registratie
COM-001	Communicatieplan

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de Cyberbeveiligingswet Toolkit · alle 50 documenten: www.maasiso.nl/toolkits/cyberbeveiligingswet/

VOORBEELD UIT DE TOOLKIT

Dit is 1 van de 50 documenten uit de Cyberbeveiligingswet Toolkit

U hebt een echt document uit de toolkit bekeken, ingevuld voor een voorbeeldorganisatie. In de toolkit zit de volledige set, in Word en Excel, klaar om aan te passen aan uw organisatie.

Wat zit er verder in

Algemeen	4
Context van de organisatie	5
Leiderschap en beleid	3
Planning, risico's en doelstellingen	5
Ondersteuning	3
Uitvoering	18
Evaluatie	3
Verbetering	1
Formulieren	8

Prijs

- € 495 excl. btw (€ 598,95 incl. btw), eenmalig
- 12 maanden updates bij wijzigingen in de norm of wet
- 30 dagen geld terug, zonder opgaaf van reden
- Op naam van uw organisatie geleverd, direct na betaling te downloaden

Direct bestellen

Bekijk alle documenten en voorbeeldpagina's
www.maasiso.nl/toolkits/cyberbeveiligingswet/

Vragen over de inhoud? Mail info@maasiso.nl.