
Procedure Incidentmelding NIS2

NIS-P01

Voorbeeldorganisatie B.V.

Procedure voor incidentmelding conform NIS2-richtlijn.

MaasISO
www.maasiso.nl

Documentinformatie

Documenttitel	Procedure Incidentmelding NIS2
Documentnummer	NIS-P01
Versie	1.0
Datum	9 oktober 2026
Auteur	[Naam contactpersoon]
Goedgekeurd door	[Naam contactpersoon]
Organisatie	Voorbeeldorganisatie B.V.
Classificatie	Vertrouwelijk

Versiehistorie

Versie	Datum	Auteur	Wijzigingen
1.0	9 oktober 2026	[Auteur]	Initiële versie

Doel

[Clausule Art. 25 t/m 29 Cbw (art. 23 NIS2-richtlijn)]

Deze procedure beschrijft de wijze waarop Voorbeeldorganisatie B.V. significante cybersecurity-incidenten meldt aan het CSIRT en de bevoegde autoriteit conform de Cyberbeveiligingswet (art. 25 tot en met 29 Cbw), de Nederlandse uitvoering van de NIS2-richtlijn. De procedure waarborgt dat de wettelijke meldtermijnen worden nageleefd: vroegtijdige waarschuwing binnen 24 uur, incidentmelding binnen 72 uur en eindverslag binnen 1 maand.

Toepassingsgebied

Deze procedure is van toepassing op alle significante incidenten die netwerk- en informatiesystemen treffen. Een incident is significant wanneer het (art. 25 lid 2 Cbw):

- Een ernstige operationele verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken; of
- Andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken

Definities en afkortingen

Term	Definitie
Significant incident	Een incident dat voldoet aan een van de criteria van art. 25 lid 2 Cbw (zie Toepassingsgebied). Nadere criteria kunnen bij algemene maatregel van bestuur worden vastgesteld (art. 25 lid 3).
CSIRT	Computer Security Incident Response Team — het CSIRT dat op grond van art. 16 Cbw voor de sector van de organisatie is aangewezen.
Bevoegde autoriteit	De toezichthouder die voor de sector van de organisatie is aangewezen op grond van art. 15 Cbw.
Vroegtijdige waarschuwing	De eerste melding aan het CSIRT en de bevoegde autoriteit, onverwijld en uiterlijk binnen 24 uur nadat de organisatie kennis kreeg van een significant incident (art. 26 Cbw).
Incidentmelding	De melding aan het CSIRT en de bevoegde autoriteit, onverwijld en uiterlijk binnen 72 uur nadat de organisatie kennis kreeg van het incident (art. 27 Cbw).
Eindverslag	Het definitieve verslag uiterlijk één maand na de melding; duurt het incident dan nog voort, eerst een voortgangsverslag en het eindverslag binnen één maand na afhandeling (art. 29 Cbw).
Tussentijds verslag	Een statusupdate op verzoek van het CSIRT of de bevoegde autoriteit (art. 28 Cbw).

Verantwoordelijkheden

Rol	Verantwoordelijkheid
Bestuur / Directie	Eindverantwoordelijkheid voor incidentmelding; besluitvorming bij escalatie; communicatie naar stakeholders; beschikbaar stellen van middelen.
CISO	Coördinatie van de incidentrespons; beoordeling significantie; uitvoeren van meldingen aan CSIRT; opstellen eindverslag; communicatie met bevoegde autoriteit.
Incidentresponsteam	Technische analyse en containment; forensisch onderzoek; herstelmaatregelen; documentatie van het incident.
IT-manager	Technische ondersteuning; monitoring van systemen; implementatie van herstelmaatregelen.
Communicatieverantwoordelijke	Communicatie naar klanten, partners en media (indien noodzakelijk).
Alle medewerkers	Onmiddellijk melden van verdachte activiteiten of incidenten aan de CISO of het incidentresponsteam.

Werkwijze

Fase 1: Detectie en interne escalatie (0-4 uur)

Bij detectie van een cybersecurity-incident worden de volgende stappen ondernomen:

- Ontdekker meldt het incident onmiddellijk aan de CISO of het incidentresponsteam
- CISO activeert het incidentresponsteam
- Initiële beoordeling: aard, omvang en potentiële impact van het incident
- Beoordeling of het incident als significant kwalificeert (meldingsplichtig)
- Bij een significant incident: directe informatie aan het bestuur
- Start van containment-maatregelen om verdere schade te beperken

Fase 2: Vroegtijdige waarschuwing — binnen 24 uur

[Clausule Art. 26 Cbw (art. 23 lid 4a NIS2-richtlijn)]

Onverwijld en uiterlijk binnen 24 uur na kennis van het significante incident stuurt de CISO een vroegtijdige waarschuwing naar het CSIRT en de bevoegde autoriteit. Deze bevat:

- Vermoedelijke aard van het incident
- Of het incident vermoedelijk door een kwaadwillende actor is veroorzaakt
- Of het incident grensoverschrijdende gevolgen kan hebben
- De contactgegevens van de functionaris die verantwoordelijk is voor de melding (art. 26 lid 2 onder c Cbw)

Fase 3: Incidentmelding — binnen 72 uur

[Clausule Art. 27 Cbw (art. 23 lid 4b NIS2-richtlijn)]

Onverwijld en uiterlijk binnen 72 uur na kennis van het significante incident stuurt de CISO een incidentmelding naar het CSIRT en de bevoegde autoriteit. Deze bevat:

- Actualisatie van de vroegtijdige waarschuwing
- Initiële beoordeling van het incident: ernst en impact
- Indicators of compromise (IoC's) indien beschikbaar

- Getroffen diensten en systemen
- Aantal getroffen gebruikers/klanten
- Genomen en geplande beheersmaatregelen

Fase 4: Tussentijdse verslagen

Op verzoek van het CSIRT of de bevoegde autoriteit worden tussentijdse statusupdates verstrekt. De CISO coördineert het opstellen en versturen van deze verslagen.

Fase 5: Eindverslag — binnen 1 maand

[Clausule Art. 29 Cbw (art. 23 lid 4d NIS2-richtlijn)]

Uiterlijk één maand na de incidentmelding stuurt de CISO een eindverslag naar het CSIRT en de bevoegde autoriteit. Duurt het incident dan nog voort, dan volgt eerst een voortgangverslag en het eindverslag binnen één maand na afhandeling (art. 29 lid 2 Cbw). Het eindverslag bevat:

- Gedetailleerde beschrijving van het incident, inclusief de ernst en de gevolgen
- Het type dreiging of de grondoorzaak die het incident waarschijnlijk heeft veroorzaakt
- Toegepaste en lopende mitigerende maatregelen
- Grensoverschrijdende gevolgen (indien van toepassing)
- Lessons learned en structurele verbetermaatregelen

Contactgegevens meldinstanties

Instantie	Contactgegevens	Meldtermijn
CSIRT (nationaal)	[URL meldportaal, in de meeste sectoren het meldportaal van het NCSC] / [telefoonnummer]	Vroegtijdige waarschuwing: 24 uur; Incidentmelding: 72 uur; Eindverslag: 1 maand
Bevoegde autoriteit	[Naam autoriteit] / [contactgegevens]	Dezelfde termijnen; de melding gaat aan het CSIRT én de bevoegde autoriteit
Autoriteit Persoonsgegevens	https://datalekken.autoriteitpersoonsgegevens.nl	Binnen 72 uur (indien ook datalek conform AVG)

[Vul de actuele contactgegevens van het nationale CSIRT en de bevoegde autoriteit in]

Communicatie naar afnemers van diensten

[Clausule Art. 30 Cbw (art. 23 lid 1 NIS2-richtlijn)]

Wanneer het significant incident gevolgen kan hebben voor de afnemers van de diensten, worden deze geïnformeerd over:

- De aard van het incident en de potentiële impact op de dienstverlening
- Maatregelen die zij zelf kunnen nemen om de gevolgen te beperken
- De verwachte hersteltijd
- Contactgegevens voor nadere informatie

Registratie

Registratie	Locatie	Bewaartermijn	Verantwoordelijke
Incidentenlogboek	SIEM / Documentbeheersysteem	Minimaal 3 jaar	CISO
Vroegtijdige waarschuwingen (kopieën)	Documentbeheersysteem	5 jaar	CISO
Incidentmeldingen aan CSIRT (kopieën)	Documentbeheersysteem	5 jaar	CISO
Eindverslagen	Documentbeheersysteem	5 jaar	CISO
Forensische onderzoeksrapporten	Documentbeheersysteem	5 jaar	CISO
Communicatie naar afnemers	Documentbeheersysteem	3 jaar	Communicatieverantwoordelijke

Verwante documenten

- NIS-001 — NIS2 Governance Document
- NIS-P02 — Procedure Ketenbeveiliging NIS2
- NIS-003 — NIS2 Risicobeheersingsmaatregelen
- PRV-P02 — Procedure Datalekken (AVG)
- Informatiebeveiligingsbeleid (indien ISO 27001 actief)