

# Procedure incidenten melden aan klanten

KET-P01

## Voorbeeld IT B.V.

*Hoe wij een incident dat een klant kan raken herkennen, de klant op tijd informeren, samenwerken bij het herstel en vastleggen wat er is gebeurd.*

## Documentinformatie

|                  |                                         |
|------------------|-----------------------------------------|
| Documenttitel    | Procedure incidenten melden aan klanten |
| Documentnummer   | KET-P01                                 |
| Versie           | 1.0                                     |
| Datum            | 16 oktober 2026                         |
| Auteur           | Sanne de Vries                          |
| Goedgekeurd door | Sanne de Vries                          |
| Organisatie      | Voorbeeld IT B.V.                       |
| Classificatie    | Intern                                  |

## Versiehistorie

| Versie | Datum           | Auteur         | Wijzigingen     |
|--------|-----------------|----------------|-----------------|
| 1.0    | 16 oktober 2026 | Sanne de Vries | Initiële versie |

[Clausule A.5.24 · A.5.25 · A.5.26 · A.5.27]

## 1. Doel

Een klant die onder de Cyberbeveiligingswet valt, moet een significant incident binnen 24 uur melden bij het CSIRT en de toezichthouder. Begint het incident bij ons, dan kan de klant die termijn alleen halen als wij snel en volledig melden. Deze procedure regelt dat.

De procedure gaat over incidenten die een klant kunnen raken: in onze eigen systemen, in de systemen van de klant die wij beheren, of bij een leverancier van ons.

## 2. Wat is een incident voor deze procedure?

Een incident is een gebeurtenis die de beschikbaarheid, de betrouwbaarheid of de vertrouwelijkheid van informatie of systemen van een klant kan aantasten. Voorbeelden:

- een aanval op onze systemen, zoals ransomware of een overgenomen account van een medewerker;
- een storing of fout bij ons waardoor een dienst voor de klant uitvalt;
- toegang tot de omgeving van een klant door iemand die daar geen recht op heeft;
- een verloren of gestolen laptop met toegang tot systemen van klanten;
- een incident bij een leverancier van ons dat gevolgen heeft voor de klant;
- een ernstig lek in software die wij voor de klant beheren of hebben ontwikkeld.

Twijfelt u of iets een incident is? Behandel het dan als incident.

## 3. Termijnen

Afspraken in het contract met de klant gaan voor. Die staan per klant in KET-005 Klanten en beveiligingsafspraken. Zonder afspraak geldt:

| Stap                        | Uiterlijk                                           | Hoe                                                                                                   |
|-----------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Eerste melding aan de klant | binnen 4 uur na ontdekking, ook buiten kantoor tijd | Telefonisch aan de contactpersoon, daarna schriftelijk met T-KET-001 Meldformulier incident aan klant |
| Update                      | elke 24 uur, en direct bij nieuwe informatie        | Schriftelijk aan het meldadres van de klant                                                           |
| Afsluitend verslag          | binnen twee weken na het herstel                    | Schriftelijk, met oorzaak en maatregelen                                                              |

## 4. Rollen

| Rol              | Taak                                                                                                         |
|------------------|--------------------------------------------------------------------------------------------------------------|
| Medewerker       | Meldt elk mogelijk incident direct bij de ISMS-coördinator.                                                  |
| ISMS-coördinator | Beoordeelt of klanten geraakt kunnen worden, doet de melding aan de klant en houdt het formulier bij.        |
| IT-beheerder     | Onderzoekt het incident, beperkt de schade en herstelt. Levert de technische feiten aan.                     |
| Directie         | Wordt bij elk incident met gevolgen voor een klant direct geïnformeerd. Besluit bij twijfel over de melding. |
| Vervanger        | Tim Hendriks, 06 23 45 67 89, als de ISMS-coördinator niet bereikbaar is.                                    |

## 5. Werkwijze

1. **Melden.** Wie iets ziet, meldt het direct bij de ISMS-coördinator: telefonisch op 030 123 45 67 of via [security@voorbeeld-it.nl](mailto:security@voorbeeld-it.nl). Noteer het tijdstip van ontdekking.
2. **Beoordelen.** De ISMS-coördinator bepaalt samen met de IT-beheerder welke klanten geraakt kunnen worden. Gebruik de klantenlijst in KET-005 Klanten en beveiligingsafspraken.
3. **Klant informeren.** Bel de contactpersoon van elke klant die geraakt kan worden. Stuur daarna het meldformulier, ook als nog niet alles bekend is. Schrijf op wat u weet en wat nog niet.
4. **Schade beperken en herstellen.** De IT-beheerder neemt maatregelen. Stem maatregelen in de omgeving van de klant af met de klant.
5. **Op de hoogte houden.** Stuur updates volgens de termijnen. Vertel ook wat de klant zelf kan doen, zoals wachtwoorden wijzigen.
6. **Afsluiten.** Stuur het afsluitende verslag met de oorzaak, de gevolgen en de maatregelen om herhaling te voorkomen.
7. **Leren.** Bespreek het incident binnen een maand intern. Neem verbeteringen op in KET-003 Basismaatregelen.

## 6. Persoonsgegevens

Zijn bij het incident persoonsgegevens van de klant betrokken en verwerken wij die in opdracht van de klant? Dan geldt ook de Algemene verordening gegevensbescherming. Als verwerker informeren wij de klant dan zonder onredelijke vertraging, zodat de klant kan beoordelen of het datalek gemeld moet worden. Volg daarvoor ook de afspraken in de verwerkersovereenkomst.

## 7. Vastleggen

Elk incident met mogelijke gevolgen voor een klant leggen wij vast met T-KET-001 Meldformulier incident aan klant, ook als het achteraf meeviel. Wij bewaren de formulieren drie jaar, tenzij een wet of contract een langere termijn voorschrijft.