

Incident-responseprocedure

Detectie, beperking, onderzoek, klantmelding, herstel en evaluatie van beveiligingsincidenten

Versie 1.0 | 7 september 2026

Meldpunt

Meld vermoedelijke beveiligingsincidenten direct via info@aireception.nl. Bij een ernstig actief incident gebruikt de klant daarnaast het afgesproken supportnummer 065 791 20 71. Deel geen gevoelige inhoud in een onbeveiligd bericht; vermeld bij voorkeur klantnaam, tijdstip, betrokken systeem en een terugbelnummer.

1. Doel en uitgangspunten

- Incidenten zo snel mogelijk herkennen, stoppen en beperken.
- Bewijs veiligstellen zonder onnodige persoonsgegevens te verspreiden.
- De klant als verwerkingsverantwoordelijke zonder onnodige vertraging informeren bij een bevestigd datalek.
- Herstel gecontroleerd uitvoeren en herhaling voorkomen.
- Alle relevante incidenten en beslissingen documenteren in een incident- of datalekregister.

2. Ernstclassificatie

Niveau	Voorbeeld	Actie
P1 - Kritiek	Actieve ongeautoriseerde toegang, grootschalige blootstelling, misbruik van API-keys of uitval van kerntelefonie.	Direct escaleren, toegang blokkeren, klant en leveranciers activeren.
P2 - Hoog	Beperkte datalekindicatie, verkeerde klanttoegang, ongeautoriseerde export of verlies van beheeraccount.	Binnen uren onderzoeken en containment uitvoeren.
P3 - Middel	Verdachte login, mislukte webhookvalidatie, beperkte configuratiefout zonder bewezen blootstelling.	Binnen één werkdag beoordelen en oplossen.
P4 - Laag	Niet-gevoelige fout, scan of mislukte aanval zonder impact.	Registreren, monitoren en meenemen in onderhoud.

3. Incidentproces

1. Ontvangst en registratie

Leg datum, melder, klant, systemen, eerste symptomen en beschikbare logs vast. Wijs een incident owner aan.

2. Eerste beveiliging

Blokkeer gestolen accounts/tokens, roteer secrets, beperk netwerk- of dashboardtoegang en zet risicovolle integraties tijdelijk uit.

3. Bewijs veiligstellen

Bewaar relevante logs, timestamps, call-ID's, configuratiewijzigingen en leveranciersmeldingen met beperkte toegang.

4. Omvang en risico beoordelen

Bepaal welke personen, gegevenscategorieën, aantallen, landen, klanten en leveranciers zijn geraakt en wat de mogelijke gevolgen zijn.

5. Klantmelding

Meld een bevestigd incident met persoonsgegevens zonder onnodige vertraging. Streeftijd: binnen 24 uur na bevestiging, waar haalbaar, zodat de klant zijn 72-uursbeoordeling kan uitvoeren.

6. Leveranciers coördineren

Open support-/securitytickets, vraag gegevensbehoud voor onderzoek waar nodig en controleer containment en verwijdering.

7. Herstel

Herstel alleen nadat toegang, secrets, configuratie en monitoring zijn gecontroleerd. Test telefonie, dashboard en meldingen.

8. Nazorg

Maak een root-cause analyse, corrigerende maatregelen, eigenaar en deadline. Informeer de klant over wezenlijke vervolgstappen.

4. Inhoud van een klantmelding

- Wat er is gebeurd en wanneer het incident is ontdekt/bevestigd.
- Welke systemen, leveranciers en klantomgevingen zijn betrokken.
- Categorieën en geschatte aantallen betrokken personen en records, voor zover bekend.
- Waarschijnlijke gevolgen en actuele risicobeoordeling.
- Maatregelen die al zijn genomen en aanbevolen acties voor de klant.
- Contactpersoon en tijdstip van de volgende update.

5. Meldingen aan toezichthouder en betrokkenen

De klant is in beginsel de verwerkingsverantwoordelijke en beslist of het datalek binnen 72 uur aan de bevoegde toezichthouder moet worden gemeld, tenzij het onwaarschijnlijk is dat het lek een risico oplevert. Bij waarschijnlijk hoog risico kan ook onverwijld communicatie aan betrokkenen nodig zijn. AI Reception ondersteunt met feiten, logs en technische maatregelen, maar neemt deze juridische beslissing niet zelfstandig namens de klant tenzij dit uitdrukkelijk is overeengekomen.

6. Incidentregister

Veld	Vastleggen
Identificatie	Incidentnummer, datum/tijd, melder, klant en incident owner.

Feiten	Systemen, gegevens, betrokkenen, omvang en tijdslijn.
Risico	Impact, waarschijnlijkheid, ernst en onderbouwing.
Acties	Containment, herstel, notificaties en leveranciersacties.
Beslissing	Waarom wel/niet gemeld aan toezichthouder/betrokkenen.
Nazorg	Oorzaak, verbetermaatregelen, eigenaar en deadline.

7. Oefenen en actualiseren

- Minimaal jaarlijks een table-top oefening of na een grote architectuurwijziging.
- Contactgegevens van leveranciers en klanten periodiek controleren.
- MFA, herstelcodes, secrets en toegangsrechten testen zonder productiegegevens te kopiëren.
- Procedure bijwerken na ieder P1/P2-incident of relevante wijziging in wetgeving/leveranciers.

Bronnen en externe documentatie

De onderstaande bronnen zijn gebruikt om de juridische en technische beschrijvingen te controleren. Leveranciers kunnen hun voorwaarden en infrastructuur wijzigen; controleer de actuele versie bij contractering.

- European Commission - Standard contractual clauses between controllers and processors: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en
- European Data Protection Board - Data breach guidance for small businesses: https://www.edpb.europa.eu/sme/assess-the-risks/data-breaches_en
- Autoriteit Persoonsgegevens - Datalek: dit moet u doen: <https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen>