Bijlage C | CIV-CARE

Incident- en Escalatieprotocol (v1.1)

Governance, veiligheid en herstel binnen casuscontext

- *Toetsingskader voor de Waardencommissie.*

---

24 DECEMBER 2025, EYGELSHOVEN

1. Doel en reikwijdte

1.1 Doel

Dit protocol beschrijft **hoe wordt gehandeld bij incidenten, signalen of overschrijdingen** binnen een CIV-CARE-casus, met als doel:

1. bescherming van betrokken personen;
2. behoud van morele en governance-legitimiteit;
3. voorkomen van machtsmisbruik, rolvervaging of datalekken;
4. herstelgericht handelen zonder straflogica.

1.2 Reikwijdte

Dit protocol is van toepassing op:

- alle werkgroepen (casussen);
- alle rollen en batches;
- alle beheerders, moderators en toezichthouders;
- alle digitale omgevingen van CIV-CARE (Web 2.0 en voorbereid op Web 3.0).

Het protocol **vervangt geen wetgeving**, maar borgt zorgvuldigheid binnen het civiel-maatschappelijk domein.

2. Definitie van een incident

Een **incident** is iedere situatie waarin sprake is van (vermoeden van):

1. overschrijding van rol- of batchgrenzen;
2. machtsconcentratie of informele hiërarchie;

3. schending van privacy of dataminimalisatie;
4. onveilige communicatie of relationele druk;
5. belangenverstrengeling;
6. misbruik van erkenning, certificaten of badges;
7. technische kwetsbaarheid met governance-impact.
8. gebruik van AI-ondersteunende systemen in strijd met het Governance-handboek, in het bijzonder:
    1. inzet van AI zonder voorafgaande validatie conform Hoofdstuk 13;
    2. inzet van AI binnen niet-toegestane batches;
    3. gebruik van AI-output als besluit, oordeel of bindend advies;
    4. ontbreken van aantoonbare menselijke besluitvorming.

❗ AI-systemen worden nimmer aangemerkt als actor; de verantwoordelijkheid ligt altijd bij de betrokken rolhouder(s).

❗ Een incident vereist **geen bewijs van schuld**, alleen een **signaal**.

3. Incidentniveaus (classificatie)

Niveau 1 – Signaal

- lichte onduidelijkheid over rol of bevoegdheid;
- onbedoelde overschrijding;
- spanningen in communicatie.

➡️ Afhandeling: **intern, laagdrempelig**.

Niveau 2 – Incident

- herhaalde roloverschrijding;
- negeren van batchbeperkingen;
- ongeautoriseerde inzage in gegevens;
- druk uitoefenen op andere deelnemers.
- inzet van AI zonder geldige governance-validatie;
- herhaald gebruik van AI in niet-toegestane batches.

➡️ Afhandeling: **tijdelijke maatregelen + toezicht**.

Niveau 3 – Ernstig incident

- structureel machtsmisbruik;

- ernstige privacy-inbreuk;
- manipulatie van governance-processen;
- weigering tot medewerking aan toezicht.
- structureel of bewust inzetten van AI ter vervanging van menselijke besluitvorming;
- negeren van AI-gerelateerde toezicht- of stopmaatregelen.

➡️ Afhandeling: **onmiddellijke escalatie**.

4. Meldingsprocedure

4.1 Wie kan melden

- iedere deelnemer;
- iedere rolhouder;
- iedere beheerder;
- leden van bestuur of commissies.

Meldingen kunnen:

- direct;
- vertrouwelijk;
- zonder formele klachtstructuur.

4.2 Hoe melden

☐ Via aangewezen meldpunt op het platform
☐ Via vertrouwelijk contact met beheerder of Waardencommissie
☐ Zonder verplichting tot identificatie (indien nodig)

Meldingen worden **nooit gebruikt tegen de melder**.

5. Eerste reactie (binnen 48 uur)

Bij iedere melding:

☐ Incident geregistreerd (zonder oordeel)
☐ Incidentniveau voorlopig vastgesteld
☐ Betrokken casus geïdentificeerd
☐ Acute risico's ingeschat

Indien nodig:
☐ Tijdelijke technische beperking toegepast
☐ Rol of batch **voorlopig gepauzeerd**

6. Escalatiestappen per niveau

6.1 Niveau 1 – Signaal

Acties:

- gesprek met betrokkenen;
- verduidelijking rol/batch;
- documentatie van leerpunt.

Geen:

- sancties;
- rolintrekking;
- publiekea registratie.

6.2 Niveau 2 – Incident

Acties:

- tijdelijke opschorting van rol of batch;
- inhoudelijke beoordeling door Waardencommissie;
- herstelgesprek (indien passend).

Verplicht:

- auditlog;
- herbevestiging of intrekking rol.

6.3 Niveau 3 – Ernstig incident

Acties (onmiddellijk):
☐ Rol en batches ingetrokken
☐ Toegang tot casus beëindigd
☐ Casus tijdelijk gepauzeerd (indien nodig)

Vervolg:
☐ Formele beoordeling Waardencommissie
☐ Inschakeling Privacycommissie (bij datalek)
☐ Advies aan bestuur over vervolg

CIV-CARE is **geen straforgaan**; bij strafbare feiten wordt verwezen naar bevoegde instanties.

6.4 AI-governance-incidenten (aanvullende bepaling)

Bij vaststelling van een AI-governance-incident gelden aanvullend de volgende maatregelen:

☐ onmiddellijke opschorting van AI-gebruik binnen de betreffende casus;
☐ vastlegging van de overtreding in het auditlog;
☐ melding aan de Waardencommissie;
☐ beoordeling of aanvullende governance-maatregelen noodzakelijk zijn.

Herstelmaatregelen mogen **niet** bestaan uit:
• verdere automatisering;
• herbeoordeling door AI;
• correctie door AI-systemen.

7. Rol van de Waardencommissie

De Waardencommissie:

- beoordeelt incidenten op **morele legitimiteit**;
- adviseert over herstel, begrenzing of uitsluiting;
- bewaakt proportionaliteit;
- voorkomt informele sanctiecultuur.

De commissie:

- heeft **geen uitvoerende macht**;
- kan **geen permanente uitsluiting** opleggen;
- adviseert altijd gemotiveerd en schriftelijk.

8. Rol van de Privacycommissie (indien van toepassing)

Bij privacy-incidenten:

☐ dataminimalisatie direct hersteld
☐ betrokkenen geïnformeerd (indien vereist)
☐ technische oorzaak geanalyseerd
☐ structurele maatregelen geadviseerd

AVG-meldingen worden alleen gedaan indien wettelijk verplicht.

9. Herstelgericht afsluiten (verplicht)

Na elk incident:

☐ Leerpunten vastgelegd
☐ Governance-maatregelen aangescherpt (indien nodig)
☐ Geen blijvende stigmatisering van betrokkenen
☐ Geen “blacklists” of verborgen labels

Herstel en begrenzing zijn leidend, **niet straf**.

10. Relatie met casusafsluiting

Een casus kan **niet definitief worden afgesloten** zolang:

☐ een incident openstaat
☐ herstelafspraken niet zijn geëvalueerd
☐ auditlog onvolledig is
☐ een vastgesteld AI-governance-incident niet is beoordeeld en afgehandeld conform dit protocol

11. Transparantie en vertrouwelijkheid

- Betrokkenen krijgen **inzage in besluiten** die hen raken;
- Details worden **niet publiek gedeeld**;
- Transparantie is contextueel, niet exposerend.

12. Slotbepaling (normatief)

Dit protocol borgt dat:

- macht altijd begrensd blijft;
- fouten bespreekbaar zijn;
- veiligheid vóór snelheid gaat;
- governance menselijk én toetsbaar blijft.

Dit protocol borgt tevens dat:

- AI nooit beslissingsmacht verkrijgt;
- menselijke regie aantoonbaar blijft;
- technologische ondersteuning ondergeschikt is aan morele en governance-afwegingen.

Het protocol is **verplicht toepasbaar** bij elke casus.

Integratie-aanwijzing

Neem dit protocol op als:

- vaste **Bijlage C** bij het Implementatiehandboek;
- verplichte **check na punt 8** in de Beheerders-checklist per casus;
- toetsingskader voor de Waardencommissie.

Opgesteld door:

Alexander Groenheide
Voorzitter | Stichting De kamer van Sociale Waarden
Menselijke waardigheid als fundament.

info@dekvsw.nl | www.dekvsw.nl
06 53 44 50 54
Laurastraat 87, 6471 JJ Eygelshoven
KVK: 97098817 | RSIN: 867909274
W: DeKvSW.nl
CIV innitiatieven:
CIV-CARE.nl | CIV-RAMP.nl | CIV-CAMP.nl | CIV-CALL.com
Burgerschapseducatie/ theater en filmeducatie: Ubuntukids.nl