AI Incident Response Procedure

SolaraCloud AI LLC — SolaraIMPACT Platform | EU AI Act & GDPR Compliance

Version 1.0 | March 2026

SECTION 1: PURPOSE AND SCOPE

This procedure establishes SolaraCloud AI LLC's response to AI-related incidents involving the SolaraIMPACT platform. It is distinct from the general security incident response (covered in the SOC 2 Type II report) and specifically addresses incidents arising from or related to AI system behaviour, AI-generated content, and AI model provider issues.

SECTION 2: DEFINITIONS

SECTION 3: INCIDENT CATEGORIES

| Category | Description | Examples |
|---|---|---|
| Category A<br>Output Quality Failure | AI-generated outputs that are factually incorrect, misleading, incoherent, or of significantly degraded quality across multiple users or modules. | Module consistently generating inaccurate market data; outputs not following module specifications; systematic hallucination of facts. |
| Category B<br>Harmful Content Generation | AI-generated outputs that contain harmful, offensive, discriminatory, or legally problematic content. | Output containing defamatory statements about real companies or individuals; discriminatory content; content promoting illegal activities. |
| Category C<br>Data / Privacy Incident | AI processing results in improper handling, exposure, or use of personal data or confidential client data. | AI output containing another client's data; model provider reports data exposure incident. |
| Category D<br>Model Provider Incident | One or more GPAI model providers (Anthropic, OpenAI, Google, xAI) reports a security incident, service disruption, or change in data handling that affects SolaraIMPACT users. | API outage; breach disclosure; policy change affecting data processing. |

| Category | Description | Examples |
|---|---|---|
| Category E<br>Regulatory / Compliance Event | A regulatory authority contacts SolaraCloud AI LLC regarding AI compliance; a legal claim is made related to AI output; a formal complaint is received regarding EU AI Act compliance. | Regulatory inquiry; lawsuit notification; formal complaint filed. |

SECTION 4: INCIDENT RESPONSE PROCEDURE

4.1 Phase 1 — Detection and Reporting (0–1 hour for P1, 0–4 hours for P2)

4.2 Phase 2 — Assessment and Classification (within 2 hours of detection for P1/P2)

4.3 Phase 3 — Containment (immediate for P1, within 4 hours for P2)

P1 containment actions may include:

- Disabling the affected AI module(s)
- Suspending API calls to the affected model provider
- Rolling back to previous module configuration
- Placing affected job outputs into review-hold status

P2/P3 containment: Flag affected outputs; notify affected users; investigate root cause.

4.4 Phase 4 — Customer and User Notification

4.5 Phase 5 — Root Cause Analysis and Resolution

For all P1/P2 incidents:

- Engineering conducts root cause analysis (RCA) within 5 business days of resolution
- RCA documents: root cause, contributing factors, timeline, resolution steps, preventive measures
- Preventive measures implemented within agreed timeframe
- RCA shared with CEO; summary available to affected customers upon request

4.6 Phase 6 — Post-Incident Review

- CEO reviews all P1/P2 incidents within 10 business days
- Monitoring Plan and incident procedures updated if gaps identified
- Annual compliance review includes summary of all incidents and near-misses

SECTION 5: INCIDENT LOG

SolaraCloud AI LLC maintains a running AI Incident Log recording:

- Incident ID, date, category, severity
- Brief description and outcome
- Regulatory reporting actions taken
- RCA completion status
- Preventive measures implemented

The log is reviewed quarterly by the CEO and forms part of the annual EU AI Act compliance file.

SECTION 6: CONTACT INFORMATION

SECTION 7: DOCUMENT CONTROL