

Incidents, concerns and remedies

What happens when an AI-supported service gets something wrong?

People need a visible route to help. The institution needs a practiced route to containment and correction.

Recommended starting position

Connect AI incidents to existing security, privacy, safety, academic and service processes. Make reporting simple, assign triage authority, preserve necessary evidence and protect affected people. Define who can pause a use and who authorizes restart.

An inaccurate answer can become an incident when it affects a deadline, eligibility or safety. A data disclosure may require a different response from an academic dispute. One visible entry point can route concerns without pretending every issue has the same owner.

What the evidence supports

Purdue directs reporting of unauthorized non-public data use. RPCC identifies reporting and investigation responsibilities. HumanSkills recommends a coordinated route that also accommodates harmful outcomes and service failures.

Establish these foundations

- Publish a reporting route that affected people can find.
- Assign triage, containment and communication responsibilities.
- Define correction, recovery and restart conditions.

The choices to make locally

Use existing incident systems

Consider this when: Existing teams can classify and route AI-related concerns reliably.

Tradeoff: Add examples and routing guidance so AI harms do not fall between categories.

Add a visible AI contact route

Consider this when: Users need a clear starting point across several kinds of concern.

Tradeoff: Connect it to responsible offices and service expectations; avoid creating an unmonitored inbox.

Suspend a use pending review

Consider this when: Continuing creates a material unresolved risk or harm.

Tradeoff: Preserve essential service, relevant evidence and a clear decision on restart or retirement.

Illustrative campus case

A student misses a deadline after incorrect advice.

An AI assistant gives an incorrect scholarship deadline. Several students may have relied on the same answer.

Fixing the answer alone does not address the students already affected.

1. Contain the faulty advice and route the issue to the accountable service owner.
2. Identify the affected scope using only necessary information and assess available remedies through authorized offices.
3. Correct the service, communicate appropriately and verify the change before unrestricted restart.

What the team produces: An incident record, affected-person response and authorized restart decision.

Who is responsible

Board and trustees: Ask how serious incidents and unresolved harms are escalated for oversight.

Institutional leaders: Assign response authority and ensure remedies and service continuity are resourced.

AI task force: Map AI concerns into existing response processes and test the handoffs.

Illustrative language to adapt

Suspected AI-related harm, information exposure, unauthorized action or material service failure must be reported through the published institutional route. Responsible offices must triage concerns, protect affected people, preserve necessary evidence and determine corrective action. Restart after suspension requires documented authorization and appropriate verification.

Read alongside model policy sections 6, 9, 11. Reconcile local authority and requirements before adoption.

Evidence of implementation

- A visible reporting route with accountable triage.
- A response exercise covering more than a cybersecurity breach.
- A record of correction, communication and restart conditions.

Reconsider when: Review after serious incidents, missed handoffs, repeated complaints or material changes to the service.

Supporting sources

[Purdue University / Artificial Intelligence Use](#)

[River Parishes Community College / Use of Artificial Intelligence](#)