

AI STRATEGY · FRAMEWORK

AI Risk and Escalation Framework

Defines how AI-related incidents and concerns get raised, escalated, and resolved.

How to use this: Adopt as-is and communicate the escalation path to all employees so no one is unsure who to tell when something looks wrong.

What Counts as an AI Incident

- ☐ An AI output was used and later found to be materially wrong or misleading
- ☐ Company, customer, or personal data was entered into a non-approved AI tool
- ☐ An AI-assisted decision (hiring, customer account action, financial) is challenged or appears biased
- ☐ A customer or partner raises a concern about AI use in the product or service

Escalation Path

Define exactly who is contacted at each stage so incidents don't stall waiting for someone to take ownership.

Who is the first point of contact for any AI-related concern raised by an employee?

Who is escalated to if the incident involves customer data or a customer-facing decision?

Who makes the final call on remediation for a significant incident (e.g. leadership, founder)?

What is the target time to first response once an incident is raised?

Incident Review and Learning

- ☐ Every significant incident is logged with what happened, impact, and resolution
- ☐ A brief review is held after significant incidents to decide if policy or process needs to change
- ☐ Patterns across incidents are reviewed quarterly alongside the other governance documents in this pack