Incident Response Plan for AI Breaches tailored for nonprofits, incorporating best practices and current guidance for AI-specific risks, compliance, and transparency:

Incident Response Plan for AI Breaches

1. Purpose & Scope

This plan outlines the procedures for detecting, responding to, and recovering from AI-related incidents (e.g., data breaches, algorithmic bias, operational failures, ethical violations) affecting [Nonprofit Name]. It ensures compliance with California and federal laws, protects stakeholders, and maintains public trust.

---

2. Roles & Responsibilities

- **Incident Response Team (IRT):**
  - IT Lead (Coordinator)
  - Data Protection Officer
  - Legal/Compliance Officer
  - Communications/PR Lead
  - AI System Owner(s)
- **Responsibilities:**
  - Lead and coordinate response
  - Assess and contain incidents
  - Communicate with stakeholders
  - Document actions and decisions

---

3. Incident Response Phases

A. Preparation

- Maintain up-to-date contact lists and secure communication channels for the IRT.
- Regularly train staff on AI risks and incident reporting.
- Conduct risk assessments and AI system audits.

B. Detection & Analysis

- Monitor AI systems for anomalies, data leaks, bias, or failures.
- Encourage staff and stakeholders to report suspected incidents promptly.
- Assess incident severity (e.g., data breach, bias, system failure) and potential impact.

C. Containment, Eradication & Recovery

- **Containment:**
    - Isolate affected AI systems or data sources to prevent further harm.
    - Apply temporary fixes or patches.
    - Secure all relevant data and logs for investigation.
- **Eradication:**
    - Remove malicious code, unauthorized access, or erroneous AI models.
    - Address vulnerabilities that enabled the incident.
- **Recovery:**
    - Restore systems and validate AI outputs.
    - Test to ensure the incident is fully resolved and systems are secure.
    - Resume normal operations.

D. Post-Incident Activity

- Conduct a debrief with the IRT to review the incident and response.
- Document the incident, actions taken, and lessons learned.
- Update policies, training, and technical safeguards as needed.
- Report to regulators and affected stakeholders if required by law (e.g., CCPA, CPRA).

---

4. Communication Protocols

- Use secure channels for internal communication during incidents.
- Notify leadership and, if required, regulatory authorities within mandated timeframes.
- Prepare public statements and FAQs for external stakeholders if the incident is public-facing.

---

5. Documentation & Reporting

- Keep detailed records of incident detection, response actions, communications, and outcomes.
- Maintain logs for compliance audits and continuous improvement.

---

6. Continuous Improvement

- Review and update this plan at least annually or after significant incidents.
- Incorporate feedback from incident reviews and new regulatory requirements.
- Conduct regular drills and tabletop exercises.

---

7. Best Practices

- Foster a culture of transparency and accountability—encourage prompt reporting without fear of blame.
- Collaborate across IT, legal, communications, and program teams.
- Leverage AI and automation for rapid detection and response when possible.
- Stay informed on evolving AI threats and regulatory changes.

References:

1 Drata – Incident Response Plan Templates

2 Wiz – Incident Response Plan Templates

5 Cimphony.ai – AI Incident Response Plans: Checklist & Best Practices

---

This template should be customized for your nonprofit's specific AI systems and reviewed by legal counsel to ensure full compliance with California and federal regulations.