DOCUMENT 3 OF 4 · AI WORKPLACE POLICY KIT

AI Incident Response Checklist

For Small Businesses

This checklist provides step-by-step guidance for responding to AI-related incidents, including data exposures, AI-generated fraud attempts, policy violations, and vendor breaches. Print and keep accessible. Complete each section in order when an incident occurs.

WHAT'S IN THIS KIT

- ✓ Incident identification and classification
- ✓ Immediate containment steps
- ✓ Data exposure response protocol
- ✓ AI fraud / deepfake response protocol
- ✓ Vendor breach response protocol
- ✓ Notification templates and documentation log

NOT LEGAL ADVICE: This document is designed for small business compliance as a starting point. Have a qualified attorney review any legal or compliance document before relying on it for legal or regulatory purposes.

aiwatchdog.com · AI Workplace Policy Kit

AI INCIDENT RESPONSE CHECKLIST

Step-by-Step Response Guide

[COMPANY NAME] · Incident Date: _____ · Incident #: _____

INCIDENT LOG — Complete at Start

Reported by (name/role)

Date and time discovered

Date and time reported to [DESIGNATED CONTACT]

Brief description of incident

Incident Type (check all that apply):

- ■ Confidential data entered into an unapproved AI tool
- ■ Client PII or sensitive data exposed to an AI tool
- ■ AI-generated phishing / fraud attempt received
- ■ AI-generated deepfake audio or video used in fraud attempt
- ■ Vendor data breach affecting an approved AI tool
- ■ Employee policy violation (unauthorized AI tool use)
- ■ AI output caused harm or error in a client deliverable
- ■ Other: _____

SECTION 1: Immediate Containment (All Incidents)

Complete these steps within the first hour of discovery:

- ■ Stop using the AI tool involved in the incident immediately.
- ■ Do not delete any evidence — preserve screenshots, emails, and logs.
- ■ Notify [DESIGNATED CONTACT] at [EMAIL/PHONE].
- ■ If client data was involved, identify which clients may be affected.
- ■ If financial accounts may be compromised, contact your bank immediately.
- ■ Document the time you completed each step above.

SECTION 2: Data Exposure Response

Complete if confidential or client data was entered into an AI tool:

- ■ Identify exactly what data was entered (type, volume, individuals affected).
  Examples: client names, email addresses, financial figures, health information, trade secrets.
- ■ Check the AI tool's data retention policy — how long is data stored?
- ■ Submit a data deletion request to the AI vendor if available.
- ■ Review whether the data is subject to breach notification requirements.
  HIPAA: notify within 60 days. CCPA: notify without unreasonable delay. GDPR: notify within 72 hours.
- ■ Consult with a qualified attorney before notifying affected individuals.
- ■ Document all steps taken and retain records for at least 3 years.

Data deletion request submitted to vendor on (date)

Attorney consulted (name/firm)

SECTION 3: AI Fraud / Deepfake Response

Complete if your business received an AI-generated fraud attempt:

- ■ Do not transfer money, share credentials, or take any requested action.
- ■ Preserve all evidence: emails, voicemails, call recordings, messages.
- ■ Verify the identity of the requester through a known, separate channel.
  Call back on a number you already have — not one provided in the suspicious message.
- ■ Report to the FBI Internet Crime Complaint Center (IC3) at ic3.gov.
- ■ If financial loss occurred, contact your bank immediately to initiate a recall.
- ■ Notify your business insurance carrier if you have a cyber or crime policy.
- ■ Alert employees about the attempt so they can watch for similar attacks.

SECTION 4: Vendor Breach Response

Complete if an approved AI vendor notifies you of a breach affecting your data:

- ■ Review the vendor's breach notification for scope and affected data types.
- ■ Assess whether your company's data or your clients' data was affected.
- ■ Change all credentials for the affected AI tool immediately.
- ■ Disable the affected tool until the vendor confirms remediation.
- ■ Follow Section 2 (Data Exposure Response) if client data was affected.
- ■ Evaluate whether to continue using the vendor after the breach.

SECTION 5: Post-Incident Documentation

- ■ Complete the Incident Log at the top of this document.

- ■ Write a brief incident summary (what happened, what data was affected, what actions were taken).
- ■ Update the Approved AI Tools List if a tool's risk level has changed.
- ■ Brief employees on the incident (without sharing unnecessary details) to prevent recurrence.
- ■ Review and update the AI Workplace Use Policy if a gap was identified.
- ■ File completed checklist in [LOCATION] and retain for at least 3 years.

Incident closed on (date)

Closed by (name/role)

NOT LEGAL ADVICE: This checklist is a starting point. Breach notification requirements vary by jurisdiction and data type. Consult a qualified attorney before notifying affected individuals or regulators. — AIWatchdog · aiwatchdog.com