ADCO AI LLC

Incident Response & Business Continuity Policy

ADCO's response to disruption must protect people, limit harm, preserve information and restore authorized work safely. This Policy establishes requirements for ADCO AI LLC and its subsidiaries and affiliated entities participating in ADCO operations, together referred to as ADCO. It applies to security, privacy and operational incidents affecting ADCO's people, information, systems or service delivery.

01 Purpose and application

Incident response and business continuity must be considered together: an outage can create privacy or security risks, and a security event can require service suspension. The objective is controlled recovery with clear accountability, timely communication and lessons applied to future work.

This public Policy sets required practices. Engagement plans must identify the actual contacts, dependencies, responsibilities and recovery arrangements appropriate to the work. It does not establish a universal recovery guarantee, response-time service level or claim that a particular exercise or restoration test has already been completed. Applicable law and agreed client obligations govern required notification and service commitments.

02 Events within scope

Covered events include suspected account compromise, phishing, malware, unauthorized access, lost or stolen equipment, exposed links, misdirected information, unapproved AI-tool use, data corruption and unauthorized changes. A personal data breach can involve loss of availability or integrity as well as disclosure, and accidental events must be assessed alongside deliberate attacks.

Continuity events include electricity or connectivity loss, provider outages, office inaccessibility, fire or other hazards, serious staffing disruption and failure of a critical dependency. A material quality defect, unsafe output or incorrect release must be escalated when it may harm a client or affected individuals. Near misses must be recorded where they reveal a meaningful weakness.

03 Response authority and functional roles

Management must designate an incident lead and an alternate appropriate to the event. The lead coordinates assessment, assigns actions and maintains a decision record. The technical owner manages system containment and restoration; the operations owner manages people, facilities and delivery; the privacy or legal function assesses notification and other legal duties; and an authorized client contact manages engagement communications.

Functions may be combined where appropriate, but responsibilities and authority must remain clear. Major shutdowns, material spending, external commitments and changes to delivery arrangements require the relevant authorized decision-maker. An unavailable manager must not prevent urgent protective action within established authority or timely escalation to an alternate.

04 Preparation and accessible response information

Project and system owners must maintain the information needed to respond: essential services, dependencies, responsible personnel and alternates, provider contacts, approved locations, access-revocation methods and client escalation requirements. Response instructions must remain accessible to authorized personnel if a usual communication or identity service fails, without exposing secrets or protected information.

Personnel must know how to recognize and report concerns, preserve relevant information and obtain direction. Preparation must consider realistic scenarios for the engagement, including misdirected data, credential compromise, loss of connectivity and unexpected unavailability of a key person. Coverage and escalation arrangements must reflect actual operating commitments.

05 Reporting and immediate protective action

Personnel must promptly report suspected incidents when discovered, including their own errors, without waiting for proof or attempting to resolve the issue silently. Reports should identify what was observed, when, the affected work or system and any immediate action taken. Good-faith reports and cooperation must be protected from retaliation.

External reports may be sent to privacy@adcohq.com or through www.adcohq.com/contact. Clients should also use agreed incident contacts. Avoid transmitting passwords or full datasets; request a secure evidence channel when necessary. For immediate threats to life or physical safety, personnel must seek appropriate local emergency assistance and follow workplace safety directions.

06 Triage, severity and escalation

The incident lead must open a record, establish ownership and assess urgency using potential harm, data sensitivity, scope, active exploitation, service interruption and legal or contractual deadlines. Uncertainty must be identified explicitly and must not be treated as evidence that no harm occurred. Severity must be reassessed as facts develop.

Critical. An ongoing serious threat to safety, extensive compromise, material exposure of sensitive information or severe disruption of critical work requires immediate management escalation and prioritized containment.

High. A credible compromise or substantial interruption with potentially significant client or individual impact requires urgent coordinated investigation and protective action.

Standard. A limited event or near miss without evidence of significant impact still requires an accountable owner, proportionate investigation and documented closure. The classification may be raised at any time.

07 Containment and harm reduction

Containment must be proportionate to the risk and coordinated with the affected system owner or client where required. Actions may include pausing processing, isolating equipment, revoking sessions or exposed credentials, restricting access, disabling public links and quarantining affected work. Safety and protection against continuing harm take priority.

Personnel must avoid actions that unnecessarily destroy evidence or broaden the incident. They must not delete relevant records, reinstall affected systems, contact an attacker or test client infrastructure without authorization. Emergency changes must be recorded and reviewed. No employee may independently agree to a ransom or other extortion demand; any proposal requires authorized management and legal assessment.

08 Evidence preservation and incident records

Relevant evidence must be preserved in a controlled location. The record should include a chronology, observations, affected resources, decisions, actions, responsible persons and communications. Timestamps must identify the relevant time zone. Original evidence should be preserved where practical, with documented handling and access sufficient to support reliable review.

Evidence collection must be lawful and proportionate and must not create an unnecessary new repository of sensitive information. Access is limited to authorized participants. Applicable legal holds must be observed, and evidence sharing must protect client confidentiality, individuals and other engagements. Operational cleanup must be coordinated with preservation requirements.

09 Investigation and impact assessment

The response team must assess the suspected cause, relevant time period, entry point, affected systems, information and people, including downstream effects on work already delivered. Investigation must consider confidentiality, accuracy, availability and possible misuse, as well as the reliability and limits of available logs or other evidence.

Known facts, reasonable assessments and unresolved questions must be distinguished. The team must identify affected clients, providers, locations and contractual obligations, and evaluate whether a security event constitutes a personal data breach. Investigation and containment may proceed together. A preliminary assessment must support timely decisions even when a final cause or full count is unavailable.

10 Client and legal notification

Where ADCO acts as a processor or subprocessor, it must notify the relevant client or upstream controller without undue delay after becoming aware of a personal data breach and meet any earlier contractual deadline. Personnel must not wait for a complete investigation or treat a controller's regulatory reporting window as permission to delay client notice. Other security or service events must be communicated as required by the agreement and their impact.

Where ADCO is responsible as controller, the privacy or legal function must assess applicable jurisdictions, thresholds and deadlines. For example, where the EU or UK GDPR applies, a notifiable breach must be reported to the competent authority without undue delay and, where feasible, within 72 hours of awareness. Affected individuals must be informed without undue delay where the applicable high-risk threshold is met, subject to lawful exceptions. Other laws may require different steps or periods.

Initial notice must provide available relevant facts, likely effects, protective actions and a contact point. Further information must follow as it becomes available without undue further delay. Notification decisions, including reasons for not notifying where appropriate, must be documented. Required disclosure must not be withheld to protect reputation or await agreement about fault.

11 Accurate and coordinated communications

The authorized communications owner must coordinate client updates with the incident lead and relevant privacy or legal support. Updates must distinguish confirmed facts from estimates, explain material changes and identify any action the recipient should take. Communication cadence must reflect severity, contractual duties and the information available.

Only authorized representatives may make public statements on ADCO's behalf. Confidentiality controls must not be used to obstruct lawful reporting, protected disclosures or required notification. Personnel must not speculate publicly about individuals or clients. Response records must preserve important decisions and communications so that later accounts remain accurate.

12 Business impact and recovery priorities

Continuity planning must identify essential work, time-sensitive obligations, data dependencies, critical providers and the consequences of interruption. Recovery priorities must consider safety, potential harm, contractual requirements and the order in which supporting systems are needed. Projects must not be prioritized solely by commercial value when another activity presents greater risk to people or information.

Where needed, engagement arrangements must define a recovery time objective, meaning the target period for restoring a service, and a recovery point objective, meaning the acceptable extent of lost recent work or data. Objectives require realistic assessment of the actual platform and responsibilities. They are not guaranteed service levels unless expressly agreed as such.

13 Continuity activation and workforce protection

Management must authorize continuity measures when normal delivery cannot safely continue. Options may include controlled suspension, reprioritization, approved alternate connectivity, reassignment to prepared personnel or an authorized alternative workspace. Clients must be informed where commitments or their instructions are affected.

Reassignment must preserve skills, supervision, access limits and quality requirements. No disruption authorizes an unapproved country, work location, subcontractor, personal account or storage service. Required client and legal approvals must precede a change. Continuity must protect employee safety and reasonable rest; recovery targets must not be met through coercive overtime, unsafe travel or excessive workloads.

14 Backup and restoration requirements

System owners must determine what information and configurations require backup, who is responsible, how copies are protected and how restoration will be verified. Backup arrangements must address access restrictions, retention, resilience against compromise of the primary environment and the sensitivity of the information involved. Where client systems control backup, ADCO must clarify dependencies rather than create unauthorized copies.

Restoration capability must be tested on a schedule proportionate to risk and after relevant material changes. The owner must record the scope, result and corrective action. The existence of a provider backup feature alone must not be treated as evidence that the required recovery outcome has been verified.

15 Controlled restoration and return to service

The responsible technical and operations owners must confirm that the immediate cause is addressed or sufficiently contained before restoration. Recovery must use approved systems and known, appropriately assessed sources. Permissions, credentials, configurations and necessary protective measures must be validated before ordinary access resumes.

Recovered work must be checked for completeness, integrity, current instructions, duplication and quality status before release. Where earlier outputs may be affected, the project owner must assess correction, replacement or client escalation. Restart authorization and unresolved risks must be recorded. Appropriate observation after recovery must check for recurrence and unexpected effects. Restoration must also reapply applicable deletion instructions and access revocations so that recovery does not reactivate information or accounts that should remain restricted or removed.

16 Exercises, lessons and corrective action

Incident and continuity arrangements must be exercised and reviewed on a risk-based schedule and after significant changes or events. Exercises should test decision-making, escalation, client communications and restoration assumptions using scenarios relevant to ADCO's work. Exercise results must not be presented as proof of capabilities outside the tested scope.

After a material incident, management must review causes, contributing conditions, response effectiveness and opportunities to prevent recurrence. Corrective actions require an owner, target completion point and verification proportionate to risk. Closure must record recovery status and residual issues. Lessons must inform training, access controls, supplier decisions and project planning rather than remain only in the incident record.

17 Governance and assurance

Executive management is responsible for maintaining accountability for this Policy. Project-specific plans must be kept current, and exceptions or material limitations must be escalated and addressed. No internal exception may waive applicable law. Changes to client obligations require a valid agreement or authorization and must remain lawful.

ADCO may provide proportionate summaries of relevant plans, exercises or corrective actions where actual records exist and disclosure is appropriate. Assurance must distinguish planned measures from implemented and tested capabilities. Sensitive response instructions, credentials, personal information and other clients' information remain protected. General questions may be submitted through www.adcohq.com/contact; security or privacy concerns may be sent to privacy@adcohq.com.