INCIDENT RESPONSE AND BUSINESS CONTINUITY OVERVIEW

ADCO AI LLC

ADCO AI LLC maintains incident response and continuity procedures designed to support prompt reporting, triage, containment, evidence preservation, impact assessment, safe recovery, client communication, corrective action, and prevention of recurrence.

1. COVERED EVENTS

Covered events include lost or stolen devices; malware, phishing, or suspected account compromise; unauthorized access; incorrect-recipient disclosure; exposed links; client information in an unapproved system; provider or connectivity disruption; office interruption; loss of key personnel; and integrity, quality, privacy, or security issues that may affect in-process or delivered work.

2. INCIDENT LIFECYCLE

- Report and triage. Open an incident record, assign responsibility, identify affected work, and prioritize according to potential impact.
- Contain. Disable accounts, revoke sessions, isolate devices, remove exposed links, pause processing, restrict access, or quarantine affected work as appropriate.
- Preserve. Retain relevant logs, files, decisions, timestamps, communications, and system evidence.
- Assess. Determine affected information, systems, people, time periods, providers, work locations, contracts, and legal or notification obligations.
- Recover. Remove the cause, restore approved service, validate access and integrity, and monitor for recurrence.
- Communicate. Notify the client and other required parties under the applicable agreement and law using confirmed facts and continuing updates where appropriate.
- Improve. Complete root-cause analysis, corrective and preventive action, management review, and evidence closure.

3. BUSINESS CONTINUITY

Project dependencies, essential roles, client contacts, approved systems, authorized work locations, and escalation paths are identified during intake to the extent appropriate to the engagement. Work may be reallocated only where the statement of work, data restrictions, access controls, quality requirements, and client instructions permit it.

Critical instructions, configuration, quality records, and access decisions are maintained in controlled systems to reduce reliance on a single person. Backup, recovery point, recovery time, restoration testing, and continuity measures are selected according to the actual platform and engagement risk; no universal recovery time is promised by this Overview.

Recovered work is not released until the applicable access, integrity, instruction version, and quality status have been validated.

4. CLIENT NOTIFICATION

Notification timing and content follow the applicable agreement, data processing terms, law, and facts reasonably available. Initial notice may be supplemented as the investigation develops. Notice does not waive legal privilege, allocate fault, or replace a later verified report.

5. EVIDENCE AND CORRECTIVE ACTION

Where appropriate and permitted, incident evidence may include a chronology, decision record, containment and access-revocation evidence, affected-system and data assessment, notification record, root-cause analysis, corrective and preventive action, recovery validation, and management closure. Evidence disclosure is subject to confidentiality, security, privacy, privilege, and the rights of other clients and individuals.

6. TESTING AND REVIEW

Incident and continuity procedures are reviewed following material changes, exercises, significant provider changes, or actual incidents. Identified gaps are assigned corrective actions and tracked to appropriate closure.

7. CONTACT

Security and privacy incidents may be reported through the contact form at adcohq.com.