ADCO AI LLC

Information Security Policy & Overview

ADCO protects the confidentiality, integrity and availability of information entrusted to its people and systems. This Policy establishes the security requirements for ADCO AI LLC and its subsidiaries and affiliated entities participating in ADCO operations, together referred to as ADCO. It applies to personnel, contractors and service providers to the extent of their responsibilities and access.

01 Purpose, scope and accountability

These requirements cover business information, personal information, client materials, credentials, work products and the systems used to support ADCO's managed human services, staff augmentation and AI operations. Protection must follow the information wherever authorized work occurs, including within client-controlled environments.

Executive management is accountable for security governance and resourcing. Designated system owners are responsible for technical safeguards; project owners for engagement-specific requirements; and operations leaders for workforce and workplace controls. Responsibilities and escalation routes must be assigned before access is provided. This public Policy describes required standards; implementation evidence and project-specific obligations are assessed separately.

02 Risk assessment and engagement readiness

Before accepting information or activating project access, the responsible owner must identify the purpose, data sensitivity, permitted users, approved tools, work locations, provider dependencies, retention requirements and client security conditions. Higher-risk activities require an appropriate assessment and additional safeguards before work begins.

An engagement must not proceed on the assumption that a capability exists because it appears in a proposal. Unmet requirements must be resolved, the scope revised, or the affected processing withheld. Material changes to data, access, delivery locations or technology require review before implementation. Risks, responsible owners and corrective actions must be recorded.

03 Information classification and minimum access

Information must be identified as public, internal, confidential or restricted according to its sensitivity and the harm that could follow misuse. Client confidentiality terms and stricter classifications take precedence. Personal information, credentials, private datasets and unpublished client outputs require controlled handling even when individual records appear ordinary.

Teams must use only the information needed for the assigned task. Masked or reduced datasets should be used where they preserve the work's purpose. Access to one project does not authorize access to another, and access to personal information does not authorize identification, contact or profiling of the individuals concerned.

04 Workforce readiness and confidentiality

Personnel must receive appropriate security, privacy and acceptable-use instruction and accept applicable confidentiality obligations before receiving client access. Project preparation must address permitted tools, sensitive content, handling restrictions, escalation and the limits of the individual's authority. Refresher instruction is required when duties, risks or requirements materially change.

Managers must verify readiness and provide supervision proportionate to experience and risk. Personnel must report suspected errors or exposure promptly and may pause unsafe processing. Good-faith reporting is protected from retaliation. Confidentiality and restrictions on retaining client information continue after a role or engagement ends.

05 Identity, authentication and access lifecycle

Access must use individually assigned accounts and documented approval. Permissions must be limited by role, project, location and duration. Multi-factor authentication is required where the system supports it, with phishing-resistant methods preferred where available. Privileged access requires separate authorization and must be limited to necessary administrative functions.

Shared user accounts and shared credentials are prohibited. Non-person service accounts require a defined owner, purpose, restricted permissions, and approved management controls. Owners must review permissions periodically and when roles or risks change. Access must be suspended or revoked promptly when it is no longer needed, including departures, project completion and suspected compromise. Account removal must include relevant sessions, tokens and shared-resource permissions.

06 Passwords, secrets and recovery information

Company credentials and recovery material must be managed through an approved company-controlled credential vault or appropriate secrets-management service. Passwords must be unique and at least sixteen characters where supported. Personnel must not reuse company passwords on personal services or approve unexpected authentication requests.

Passwords, API keys and recovery codes must not be stored in ordinary messages, spreadsheets, source code or project deliverables. Secrets must be shared only through an approved method with authorized recipients. Suspected exposure requires immediate escalation, proportionate credential rotation, session or token revocation and review of affected access.

07 Devices and endpoint protection

Devices authorized to process client information must use supported operating systems, security updates, active platform-native or approved endpoint protection, automatic screen locking and authentication on resume. Full-disk or equivalent encryption is required for devices approved to hold client information. Administrative privileges must be restricted and unnecessary software removed or disabled.

Devices must remain under accountable control and be stored securely when unattended. Personal devices, removable media, local downloads and printing require express approval under the engagement's rules; convenience does not authorize them. Lost, stolen, tampered-with or unexpectedly behaving equipment must be reported promptly and withheld from sensitive work until assessed.

08 Physical security and authorized workplaces

Work involving protected information must take place only in approved locations with physical conditions suitable for the task. Workplace controls must address access by visitors and unauthorized personnel, secure equipment storage, screen visibility, confidential conversations and disposal of paper records. Visitors must not be given incidental access to client systems or materials.

Remote work and relocation require the same attention to access, privacy and client restrictions as office work. Personnel must not photograph screens, record client work or allow household members or other third parties to view it without authorization. Safety incidents and loss of physical control over equipment require escalation.

09 Approved systems, AI tools and communications

Client information may be processed only within client systems or expressly approved ADCO-managed systems and communication channels. Personal email, personal cloud storage, consumer messaging, public AI tools and unapproved web applications must not receive client information. Approval must cover the specific tool, account, purpose and data involved.

This restriction includes assistants, translation services, transcription tools, browser extensions and automated integrations that can transmit information to another provider. Authorized AI assistance must follow the client's instructions and any restrictions on model training, retention or provider access. Personnel must not substitute automation for required human work or silently use a tool to complete an assessment.

10 Storage, transmission and geographic restrictions

Protected information must use approved encrypted connections in transit and access-controlled storage with encryption appropriate to its sensitivity. Encryption keys and administrative access must be protected separately from routine user permissions where the system permits. Public sharing links and unnecessary copies are prohibited for confidential client information.

Recipients, permissions and destination must be checked before transfer. Cross-border access, cloud-region changes and movement between affiliated entities remain subject to client instructions and applicable legal safeguards. Data residency or localization requirements must be established during intake; a disruption or staffing shortage does not independently authorize a transfer.

11 Application and change security

ADCO-controlled applications and integrations must be designed and configured to enforce authorization at the appropriate service or database layer, protect stored information and use encrypted transport. Client separation must not depend solely on what a user interface displays. Administrative actions require role restrictions and appropriate accountability.

Material changes must be reviewed for security and privacy impact and tested before release, with a recovery approach proportionate to the change. Dependencies and configurations must be maintained. Test environments should use synthetic or appropriately protected data. Client information must not be placed in source repositories or development tools without explicit authorization.

12 Logging, detection and vulnerability management

System owners must define appropriate records of access, administrative actions, significant changes and security events. Logs must be protected against inappropriate access or alteration, reviewed according to risk and retained for a justified period. Logging must minimize unnecessary personal information and must not deliberately capture passwords or unrestricted sensitive payloads.

Security weaknesses must be assessed and prioritized according to exploitability, exposure, affected information and business impact. Owners must assign remediation, apply urgent containment where necessary and verify corrective action. Monitoring must be proportionate and lawful, with required workforce notices. Personnel must not conduct unauthorized scans, penetration tests or experiments against client systems.

13 Service providers and subcontractors

Providers with access to protected information must be assessed for their role, security responsibilities, data handling, subprocessors and recovery dependencies before use. Appropriate contracts must address confidentiality, permitted processing, security, incident assistance and return or deletion. Required client approval must be obtained before introducing or materially changing a provider.

ADCO personnel must not delegate client work to undisclosed freelancers or outside parties. Affiliation alone does not authorize data access. Provider security reports may support diligence but do not establish that ADCO itself holds the provider's certification or that every proposed workflow is covered.

14 Retention, return and secure disposal

Information must be retained only for an authorized purpose and for the period required by applicable instructions, law or legitimate operational need. Project closure must include review of access, active copies, shared links and agreed return or deletion tasks. Devices and media must be securely erased or destroyed before disposal or reuse where protected information may remain.

Legal holds and permitted backup retention must be documented and limited. Information retained under an exception must remain protected and unavailable for unrelated use. Deletion statements must accurately describe the systems and copies addressed and any justified limitations; they must not imply removal from systems outside ADCO's control. Moving a record to trash or hiding it from ordinary view is not secure erasure; restricted recoverable copies remain subject to retention and access controls.

15 Incident response and continuity

Suspected unauthorized access, loss, disclosure, malware, integrity failure or security bypass must be escalated and assessed under ADCO's Incident Response & Business Continuity Policy. Response must prioritize safety, containment, evidence preservation and timely communication. Required client or regulatory notices must not be postponed until a complete investigation is available.

Continuity arrangements must preserve security during disruption and restoration. Backup responsibilities, recovery priorities and restoration checks must be defined for the relevant systems and engagement. Recovered work requires validation of access, integrity and quality before release. Specific service levels and recovery commitments belong in the applicable agreement.

16 Review, exceptions and responsible assurance

Control owners must review these requirements periodically and after significant changes or incidents. Exceptions require documented justification, risk assessment, accountable approval, compensating safeguards and a review or expiry point. No internal exception may waive applicable law. Changes to client obligations require a valid agreement or authorization and must remain lawful. Material gaps must lead to corrective action or restricted processing.

ADCO's assurance statements must distinguish policy requirements, implemented controls and independently verified evidence. No certification or audit status may be claimed unless current and substantiated. Proportionate evidence may be shared under appropriate confidentiality arrangements while protecting sensitive security details, personal information and other clients.

17 Security inquiries and reporting

Security concerns and suspected privacy incidents may be reported to privacy@adcohq.com. General security and assurance inquiries may also be submitted through www.adcohq.com/contact. Include a short description, the affected service and a way to contact you. Do not send passwords, full datasets or unnecessary personal information; request an appropriate secure channel for sensitive evidence. Clients should also use the incident contacts specified in their agreements.