CLIENT INFORMATION SECURITY OVERVIEW

ADCO AI LLC

ADCO AI LLC applies administrative, technical, organizational, workforce, and physical safeguards designed to protect client information throughout authorized service delivery. Controls are applied according to the engagement scope, data classification, contractual requirements, approved systems, and documented client instructions.

1. SECURITY GOVERNANCE

Security requirements are identified during engagement intake and incorporated into project instructions, access decisions, and applicable agreements. Access is a revocable business authorization and is reviewed when roles, projects, systems, risk, or personnel change. Material issues are documented, escalated, corrected, and reviewed for recurrence prevention.

2. IDENTITY AND ACCESS MANAGEMENT

- User identity. Client systems and ADCO-controlled project systems use named, invitation-only accounts. Shared user accounts are prohibited unless a client system technically requires them and equivalent accountability controls are approved.
- Authentication. Multi-factor authentication is required before authorized access is activated where the system supports it. Authenticator applications or security keys are preferred where available.
- Authorization. Access is limited by role, project, business need, approved location, and engagement period. Privileged functions are reserved for specifically authorized administrators.
- Lifecycle. Access follows documented request, approval, provisioning, review, role-change, suspension, and revocation procedures. Access is revoked promptly when no longer required.

3. CREDENTIALS AND SECRETS

Company-owned credentials and recovery material are maintained in a company-controlled credential vault. Unique passwords of at least sixteen characters are required where supported, and credential reuse is prohibited. Credentials, recovery codes, and application secrets may not be stored in ordinary email, chat, spreadsheets, tickets, or source code. Suspected exposure triggers reset, session revocation, access review, and incident assessment.

4. APPROVED DEVICE BASELINE

- Encryption. Full-disk or equivalent device encryption is required for devices approved to process client information.
- Screen protection. Automatic screen locking and authentication on resume are required.
- Updates. Approved devices must use a supported operating system with security updates enabled and critical updates applied promptly.
- Endpoint protection. Platform-native or approved endpoint protection must remain active and current.
- Account separation. Named user profiles and restricted administrative privileges are used where practical.
- Physical control. Devices must be stored securely, protected from unattended public use, and reported immediately if lost or stolen.

5. DATA PROTECTION AND APPROVED CHANNELS

Client information is classified, minimized, and limited to the approved purpose. Approved services use encrypted network connections and private, access-controlled storage. Unnecessary local downloads are minimized. Client information may be processed only through the client system, an approved ADCO-controlled system, company-managed storage, or company-managed email when the engagement permits it.

Personal email, personal storage, consumer messaging applications, removable media, public artificial-intelligence tools, and unapproved web applications are prohibited for client information. Information is processed only from authorized, client-approved work locations.

6. APPLICATION AND PLATFORM CONTROLS

ADCO-controlled applications use encrypted transport, access-controlled storage, role-based behavior, database authorization controls, security headers, and audit events appropriate to the system. Administrative workflows are role-limited and authorization-tested. Source code repositories exclude client data unless the client expressly authorizes otherwise.

7. WORKFORCE AND THIRD-PARTY CONTROLS

Authorized personnel are bound by confidentiality, acceptable-use, information-security, data-protection, and intellectual-property obligations. Access is limited to assigned work. Client information is not disclosed to undisclosed freelancers or subcontractors. Service providers are reviewed according to their role, contractual terms, data involvement, and engagement requirements.

8. INCIDENT RESPONSE

Suspected loss, unauthorized access, malware, disclosure, integrity failure, or policy bypass is reported, triaged, and contained. ADCO preserves relevant evidence, assesses affected information and obligations, eradicates the cause, recovers through approved systems, validates controls, documents corrective action, and notifies the client within the period required by contract or law using the facts reasonably available.

9. ASSURANCE

ADCO may provide proportionate policy excerpts and control evidence under a nondisclosure agreement or defined audit protocol while protecting credentials, sensitive logs, personal information, system security, and information concerning other clients. ADCO does not claim current SOC 2 or ISO/IEC 27001 certification.

10. CONTACT

Security inquiries may be submitted through the contact form at adcohq.com.