Security Policy

Data protection, access control, platform security, incident response, and compliance at AdManage.ai.

Version	2.0
Last updated	21 August 2026
Owner	Security Team / Data Protection Officer
Contact	security@admanage.ai

Shared for vendor security review. The current version of this document is always published at admanage.ai/security-practices.

1. Security Overview

At AdManage.ai, security is paramount. We implement industry-leading security measures to protect your data, advertising accounts, and campaigns across Meta (Facebook & Instagram), TikTok, and Google Ads platforms. This policy outlines our comprehensive security framework and your role in maintaining account security.

2. Data Protection & Encryption

End-to-End Encryption

- All data transmitted between your browser and our servers uses TLS 1.3 encryption
- API communications with Meta, TikTok, and Google platforms use OAuth 2.0 secure protocols
- All authentication tokens and API keys are encrypted using AES-256 encryption
- Sensitive data is encrypted at rest using AES-256 encryption
- All URLs must use HTTPS protocol for secure communication

Data Storage & Infrastructure

Your advertising data is securely stored and managed using:

- **PlanetScale:** Serverless MySQL database platform with automatic backups and encryption
- **Railway:** Secure cloud hosting platform for our application servers
- End-to-end encryption for all data in transit and at rest
- Automated backup systems with point-in-time recovery
- Geographic redundancy and high availability
- Regular security updates and patches

3. Information Security & Risk Management

Information Security Policy

AdManage.ai maintains a formal Information Security Policy that governs all aspects of information security across the organisation.

- Comprehensive Information Security Policy documented and communicated to all employees
- Annual policy review and update process to address emerging threats and regulatory changes
- Security policies aligned with industry best practices and regulatory requirements

Risk Management

- Regular risk assessments to identify, evaluate, and prioritise information security risks
- Risk treatment plans developed and implemented for identified risks
- Continuous monitoring of risk landscape and threat intelligence
- Risk register maintained and reviewed periodically

Internal Audits

- Annual internal security audits conducted
- Audit findings tracked and remediated
- Continuous improvement based on audit recommendations

Personnel Security

- **Background Verification:** Background checks conducted for all employees and contractors prior to employment
- **Confidentiality Agreements:** All employees and contractors sign NDAs and confidentiality agreements
- **Security Awareness Training:** Mandatory security awareness training for all personnel upon onboarding and annually thereafter

- **Role-Based Access:** Access to systems and data granted based on job responsibilities

4. Advertising Platform Security

Meta (Facebook & Instagram) Integration

- ✓ OAuth 2.0 authentication - we never store your Meta passwords
- ✓ Limited scope permissions - only access what's needed for ad management
- ✓ Automatic token refresh with encrypted token storage
- ✓ Compliance with Meta's Platform Terms and Data Use Policy
- ✓ Real-time monitoring of API access and usage

TikTok Ads Manager Integration

- ✓ TikTok Marketing API secure authentication
- ✓ Granular permission controls for ad account access
- ✓ Encrypted storage of TikTok Business Center credentials
- ✓ Compliance with TikTok Ads API Terms of Service
- ✓ Audit logs for all campaign creation and modification activities

Google Ads Integration

- ✓ Google OAuth 2.0 secure authentication
- ✓ Compliance with Google Ads API Terms of Service
- ✓ Encrypted storage of Google Ads credentials
- ✓ Audit logs for all Performance Max campaign activities

5. Access Control & Authentication

Passwordless Authentication

- Google OAuth 2.0 single sign-on (SSO)
- Magic link / OTP authentication via email
- WorkOS SSO for eligible enterprise organisations
- MFA available via Google / IdP when organisation-enforced
- No customer password authentication in production
- Session timeout after inactivity
- Secure token-based authentication

Team Access Management

- Role-based access control (RBAC)
- Granular permissions for team members
- Activity logs and audit trails
- Immediate access revocation capability

Privileged Access Management

- Privileged access controls for administrative functions
- Principle of least privilege enforced across all systems
- Regular access reviews and certification
- Separate accounts for administrative tasks

6. Asset Management

Asset Inventory

- Comprehensive inventory maintained of all assets involved in service provision
- Assets classified based on sensitivity and criticality
- Regular asset inventory reviews and updates
- Clear ownership assigned for all information assets

Device & Storage Policies

- **No BYOD Policy:** Personal devices are not permitted for processing sensitive customer data
- **External Storage Prohibited:** External storage devices (USB drives, external hard drives) are not permitted for storing company or customer data
- All company data must reside on approved, secured cloud infrastructure

7. Physical & Environmental Security

Remote-First Company Model

AdManage.ai operates as a remote-first company with no physical data centres or offices housing customer data.

- All infrastructure hosted by certified cloud providers (Railway, PlanetScale, Google Cloud)
- Cloud providers maintain SOC 2 Type II, ISO 27001, and other relevant certifications
- No physical servers or data storage on premises
- Employee workstations do not store customer data locally

Physical Meeting Security

- Guest access policies in place for any physical meetings
- Visitors must be accompanied by authorised personnel
- No customer data accessed or displayed during physical meetings without appropriate controls

8. Third-Party/Vendor Management

Vendor Risk Assessment

- Formal vendor risk assessment process for all third-party service providers
- Security requirements included in vendor contracts
- Regular review of vendor security posture
- Right to audit clauses in agreements with critical vendors

Sanctions Compliance

- Controls in place to ensure compliance with applicable sanctions regulations
- Vendor screening against sanctions lists
- Ongoing monitoring for sanctions-related risks

Sub-Processors & Infrastructure Partners

The following sub-processors are authorised to process data on behalf of customers:

PlanetScale Inc. (USA) - Database hosting and management
SOC 2 Type II certified, encryption at rest and in transit

Railway Corp. (USA) - Application hosting
SOC 2 Type II certified, isolated container environments

Google Cloud Platform (USA/EU) - BigQuery data warehousing, Gemini AI services
SOC 1/2/3, ISO 27001, ISO 27017, ISO 27018 certified

Cloudflare Inc. (USA) - CDN and media storage (R2)
SOC 2 Type II, ISO 27001 certified

Upstash Inc. (USA) - Redis caching services
SOC 2 Type II certified, data encrypted at rest

Stripe, Inc. (USA) - Subscription billing and payment processing
PCI DSS Level 1, SOC 2 Type II; card details never touch AdManage servers

Resend (USA) - Transactional email delivery
SOC 2 Type II

Functional Software, Inc. (Sentry) (USA) - Application error monitoring
SOC 2 Type II

PostHog, Inc. (USA/EU) - Product analytics
SOC 2 Type II

9. Campaign & Ad Security

Secure Ad Launch Process

- **URL Validation:** All destination URLs must use HTTPS protocol
- **Content Validation:** Upload type/size validation, HTTPS-only destination URL checks, and advertising-platform policy enforcement
- **Approval Workflow:** Multi-step approval process for campaign launches
- **Budget Controls:** Spending limits and alerts to prevent unauthorised spending
- **Creative Protection:** Secure storage and delivery of ad creatives

Security Requirements for Ads

- All landing pages must use HTTPS (not HTTP)
- No links to known phishing or malware sites
- Compliance with platform policies (Meta, TikTok, Google)
- Regular security scans of linked domains

10. Data Processing & GDPR

Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") forms part of the agreement between AdManage.ai ("Processor") and the customer ("Controller") for the provision of advertising management services.

1. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person as defined in GDPR Article 4(1).

"Processing" means any operation performed on Personal Data as defined in GDPR Article 4(2).

"Sub-processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

2. Scope and Purpose of Processing

Subject Matter: Provision of advertising campaign management services across Meta, TikTok, and Google Ads platforms.

Duration: For the term of the service agreement plus any retention period required by law.

Nature & Purpose: Storage, transmission, and management of advertising campaign data; performance analytics; media processing; automation execution.

Types of Personal Data: Business contact information (name, email), advertising account identifiers, campaign performance metrics (aggregated).

Categories of Data Subjects: Controller's employees and authorised users of the AdManage.ai platform.

3. Processor Obligations

Process Personal Data only on documented instructions from the Controller, unless required by law.

Ensure persons authorised to process Personal Data are bound by confidentiality obligations.

Implement appropriate technical and organisational security measures as described in this Security Policy.

Assist the Controller in responding to data subject requests (access, rectification, erasure, portability).

Delete or return all Personal Data upon termination of services, at the Controller's choice.

Make available all information necessary to demonstrate compliance and allow for audits.

Notify the Controller without undue delay (within 72 hours) upon becoming aware of a Personal Data breach.

4. Sub-processors

The Controller provides general authorisation for the Processor to engage sub-processors as listed in Section 8 (Third-Party/Vendor Management).

The Processor shall inform the Controller of any intended changes to sub-processors, providing the Controller an opportunity to object.

5. International Data Transfers

Where Personal Data is transferred outside the EEA, the Processor ensures appropriate safeguards are in place, including:

EU-US Data Privacy Framework certification (where applicable)

Standard Contractual Clauses (SCCs) approved by the European Commission

Supplementary measures including encryption in transit and at rest

6. Security Measures

The Processor implements the technical and organisational measures detailed in this Security Policy, including:

AES-256 encryption at rest and TLS 1.3 encryption in transit

OAuth 2.0 / SSO passwordless authentication (no customer password store in production)

Role-based access control and audit logging

Regular security assessments and vulnerability scanning

24-hour disaster recovery capability

7. Data Subject Rights

The Processor shall assist the Controller in fulfilling obligations to respond to data subject requests for:

Access to their Personal Data

Rectification of inaccurate data

Erasure ("right to be forgotten")

Restriction of processing

Data portability

Objection to processing

8. Data Retention and Deletion

Personal Data is retained for the duration of the service agreement.

Upon termination, all Personal Data will be deleted within 30 days, unless retention is required by law.

The Controller may request earlier deletion or return of data at any time.

Backups containing Personal Data are purged within 90 days of deletion.

9. Audit Rights

The Controller has the right to audit the Processor's compliance with this DPA. Audits may be conducted:

Upon reasonable notice (minimum 30 days)

During normal business hours

No more than once per calendar year (unless a breach has occurred)

At the Controller's expense

10. Liability

Each party's liability under this DPA is subject to the limitations set forth in the main service agreement. The Processor shall be liable for damages caused by processing that infringes GDPR or this DPA.

By using AdManage.ai services, the Controller agrees to this DPA. For a signed copy or custom DPA requirements, contact **security@admanage.ai**.

Data Controller vs. Data Processor

AdManage.ai acts strictly as a Data Processor under GDPR and equivalent data protection regulations.

- **You (the customer)** are the Data Controller, determining the purposes and means of processing your advertising data
- **AdManage.ai** processes your data solely on your behalf and according to your instructions
- We do not determine the purposes of processing or use your data for our own independent purposes
- We do not act as a Joint Controller with our customers

Scope of Data Processing

Audience/End-User Data

AdManage.ai does not process individual personal data of your ad viewers or audience members.

- We do not receive or store personal data of individuals who view or interact with your ads

- Audience targeting parameters are passed through to Meta/TikTok/Google without algorithmic analysis
- Performance metrics we display (age groups, countries, devices) are pre-aggregated by the advertising platforms - we do not receive or process raw user-level data

Processing we perform on **your business data** (creative assets and campaign configuration):

AI-Assisted Creative Naming

Vision AI analyzes your creative content (videos/images) for categorisation and naming standardisation. This helps organise your assets with consistent naming conventions.

Performance Analytics

Aggregation and calculation of ad performance metrics (CTR, CPC, ROAS, etc.) from pre-aggregated platform data for your reporting dashboards.

Media Optimisation

Video and image processing (format conversion, thumbnail generation, dimension optimisation) to ensure platform compliance and optimal delivery.

Automation Execution

Rule-based automation for budget adjustments and status changes based on performance thresholds you configure.

All processing is performed solely to deliver our ad management services to you and is not used for any independent purposes.

11. AI Usage & Responsible AI

Third-Party AI Services

AdManage.ai uses third-party AI services to enhance our platform capabilities:

Google Gemini

Used for: Creative content analysis, naming suggestions, and text generation

Security assessment: Google Cloud maintains SOC 1/2/3, ISO 27001, and other certifications

Data processing agreement in place with Google

Customer Data & AI

- ✓ **No AI Training:** Customer data is never used to train AI models
- ✓ **No Prompt Retention:** Customer prompts and AI outputs are not retained by default
- ✓ **Transient Processing:** AI interactions are processed in real-time and not stored for future model improvement

AI Security Guardrails

- **Prompt Injection Protection:** Input validation and sanitisation to prevent prompt injection attacks
- **Content Filtering:** Output filtering to prevent generation of harmful or inappropriate content
- **Rate Limiting:** AI request rate limiting to prevent abuse
- **Input Validation:** Strict validation of all inputs sent to AI services

12. Privacy & Compliance

Data Privacy Compliance

- GDPR compliant (European Union)
- Regular privacy impact assessments

Security Standards

- Industry best practices for web application security
- OWASP Top 10 security guidelines
- Regular security assessments and code reviews
- Secure development lifecycle (SDLC) practices
- Dependency vulnerability scanning

Data Protection Officer

For data protection enquiries, please contact our Data Protection Officer at: security@admanage.ai

Data Breach Notification

In the event of a personal data breach, AdManage.ai will notify affected customers within 72 hours of becoming aware of the breach, as required by GDPR Article 33.

Anti-Bribery & Anti-Corruption

AdManage.ai maintains an anti-bribery and anti-corruption policy. We are committed to conducting business ethically and in compliance with all applicable anti-bribery and anti-corruption laws and regulations.

Modern Slavery Statement

AdManage.ai is committed to preventing modern slavery and human trafficking in our operations and supply chain. We expect our suppliers and partners to share this commitment and maintain appropriate policies and procedures.

13. Network Security

Firewall & Traffic Filtering

- Web Application Firewall (WAF) filtering all incoming traffic
- Outbound traffic filtering and monitoring
- Annual firewall rule review process
- Documented network security architecture

Intrusion Detection & Prevention

- Intrusion Detection Systems (IDS) monitoring for suspicious activity
- Intrusion Prevention Systems (IPS) to block malicious traffic
- Real-time alerting for security events
- Regular review of detection rules and signatures

DDoS Protection

- Cloudflare DDoS protection for all web traffic
- Rate limiting to prevent abuse
- Traffic analysis and anomaly detection

14. Endpoint Security

Workstation Security

- Anti-malware solution required on all company workstations
- Automatic security updates enabled
- Full disk encryption required
- Screen lock policy enforced

Device Security Policies

- Security configuration baseline for all devices
- Regular security patching and updates
- Remote wipe capability for lost or stolen devices
- Device inventory and tracking

15. Vulnerability Management

Vulnerability Management Programme

- Regular vulnerability scanning of infrastructure and applications
- Dependency vulnerability scanning in CI/CD pipeline
- Risk-based prioritisation of vulnerability remediation
- Tracking and reporting of vulnerability metrics

Customer Communication

For critical vulnerabilities that may affect customer data or service availability:

- Timely communication to affected customers
- Clear description of the issue and remediation steps
- Status updates until resolution

Responsible Disclosure

We maintain a responsible disclosure programme for security researchers. Please report vulnerabilities to **security@admanage.ai**.

16. Independent Penetration Testing

AdManage.ai is assessed by an independent security consultant who performs penetration testing against our production platform and reviews our application, infrastructure, and access controls. Findings are triaged, remediated according to the severity timelines in Section 15, and re-tested before closure.

Requesting the report

The full penetration test and security audit report is available to customers and prospects completing a vendor security review. Because it contains detailed findings, the report is hosted behind a password:

- **Report location:** admanage.ai/security-audit
- **Access:** email security@admanage.ai to request the password. We will share it directly with you, along with a signed copy or a copy under NDA if your review requires one.
- **Confidentiality:** the report and its password are shared for your internal vendor assessment only and should not be redistributed.

Open the report to download the PDF

17. Log Management

Log Management Policy

AdManage.ai maintains comprehensive logging to support security monitoring, incident investigation, and compliance requirements.

- Centralised log collection and storage
- Log retention in accordance with regulatory requirements
- Regular log review and analysis

Log Contents

Security logs capture:

- **Timestamp:** When the action occurred (UTC)
- **Action:** What action was performed
- **User:** Who performed the action
- **Result:** Success or failure of the action
- **Resource:** What resource was affected

Employee Action Logging

All employee actions on client data are logged and auditable. This includes data access, modifications, and administrative actions.

Log Security

- Logs encrypted in transit using TLS
- Access to logs restricted to authorised security personnel
- Log integrity protection to prevent tampering

18. System Hardening

Infrastructure Hardening

- Security baseline configurations for all systems
- Removal of unnecessary services and software
- Secure configuration of operating systems and applications
- Regular hardening reviews and updates

Port & Service Management

- Only necessary ports and services enabled
- Annual review of open ports and running services
- Documentation of all exposed services and their purposes
- Closure of unused ports and services

19. Secure Software Development

Secure Development Lifecycle (SDLC)

- Formal SDLC methodology with security integrated at all phases
- Annual review of SDLC processes and security practices
- Security requirements defined during design phase
- Threat modelling for new features

Environment Separation

Strict separation between environments:

- **Development:** For active development work
- **Testing/Staging:** For QA and pre-production validation
- **Production:** Live customer-facing environment

Customer data is never used in development or testing environments.

Security Testing

- **Static Application Security Testing (SAST):** Automated code analysis for vulnerabilities
- **Dynamic Application Security Testing (DAST):** Runtime security testing
- **Dependency Scanning:** Automated scanning for vulnerable dependencies
- **Pre-Release Security Review:** Security testing before production deployment

OWASP Top 10 Protections

Protection against common web application vulnerabilities:

- SQL Injection protection via parameterised queries
- Cross-Site Scripting (XSS) prevention
- Cross-Site Request Forgery (CSRF) tokens
- Input validation and output encoding
- Secure session management

Version Control & Change Management

- All code changes tracked in version control (Git)
- Code review required before merge
- Automated testing in CI/CD pipeline
- Audit trail of all changes

20. Change Management & Deployment Security

Three-Environment Architecture

All changes to AdManage.ai follow a strict deployment pipeline through isolated environments:

1. Testing Environment

- Isolated development and QA testing
- Automated unit and integration tests
- Security vulnerability scanning
- Performance benchmarking

2. Staging Environment

- Production-mirror configuration
- User acceptance testing (UAT)
- Final security validation
- Load and stress testing

3. Production Environment

- Live customer-facing platform
- Blue-green deployment strategy
- Instant rollback capability
- Real-time monitoring and alerts

Change Control Process

1. **Automated Testing:** Must pass all test suites (unit, integration, E2E)

Security Controls

- Code signing and integrity verification
- Secrets management via environment variables
- Audit logging for all deployments
- Automated rollback on failure

21. Business Disaster Recovery Plan

24-Hour Recovery Guarantee

AdManage.ai maintains a comprehensive disaster recovery plan ensuring full service restoration within 24 hours or less for any incident, including:

- Complete system failures
- Data centre outages
- Cyber security incidents
- Natural disasters
- Platform-wide service disruptions

Backup Strategy

- **Real-time replication:** Continuous data sync
- **12 hour snapshots:** Point-in-time recovery
- **Daily backups:** Full database exports
- **Geographic redundancy:** Multi-region storage
- **30-day retention:** Historical data recovery

Recovery Infrastructure

- **PlanetScale:** Automated failover & backups
- **Railway:** Multi-region deployment ready
- **CDN assets:** Globally distributed
- **API redundancy:** Load-balanced servers
- **Code repository:** Version-controlled recovery

Recovery Time Objectives (RTO)

Critical Services (Auth, API):	**< 2 hours**
Ad Campaign Management:	**< 4 hours**
Analytics & Reporting:	**< 8 hours**
Full Platform Restoration:	**< 24 hours**

Disaster Recovery Procedures

1. **Immediate Response (0-60 min):**
   - Incident detection and alert team activation
   - Initial assessment and severity classification
   - Activate disaster recovery team
2. **Data Recovery (1-4 hours):**
   - Restore from most recent backup
   - Verify data integrity and consistency
   - Synchronise with Meta, TikTok, and Google platforms
3. **Full Restoration (4-24 hours):**
   - Complete system functionality verification
   - Performance optimisation and monitoring
   - Post-incident review and documentation

Data Protection Guarantees

✓ **Zero Data Loss:** Maximum 1 hour of data at risk (RPO)

✓ **Campaign Continuity:** Active campaigns continue running

✓ **Budget Protection:** No unauthorised spending during recovery

✓ **API Connectivity:** Meta, TikTok & Google connections maintained

Communication During Disasters

Status Page: status.admanage.ai for real-time updates

Support: Available Monday-Friday during UK business hours

Account Managers: Direct contact for enterprise clients

Testing & Validation

Our disaster recovery plan undergoes:

- Annual compliance check and validation

22. Business Continuity Plan

Continuity Objectives

Our Business Continuity Plan ensures AdManage.ai maintains critical operations during any disruption:

- Maintain 99.9% uptime for ad campaign operations
- Zero interruption to active advertising campaigns
- Continuous access to campaign analytics and reporting
- Uninterrupted API connectivity with Meta, TikTok, and Google
- Customer support availability (Monday-Friday, UK business hours)

Business Functions Priority

1. **Critical:** Ad serving & campaign management
2. **Critical:** Payment processing & billing
3. **High:** Customer authentication & access
4. **High:** Real-time analytics & reporting
5. **Medium:** New campaign creation
6. **Low:** Historical data exports

Team Continuity

- Remote work capability for all staff
- Cross-trained backup personnel
- On-call rotation schedule during business hours
- Documented escalation procedures
- Emergency contact database
- Virtual collaboration tools ready

Operational Redundancy

Infrastructure Redundancy

- Multi-region deployment across 3+ zones
- Automatic failover between regions

- Load balancing across multiple servers
- Redundant API endpoints
- Multiple CDN providers

Data Redundancy

- Real-time database replication
- Geographically distributed backups
- Point-in-time recovery capability
- Offline backup archives
- Encrypted backup storage

Continuity Scenarios & Response

Scenario 1: Partial Service Outage

- Automatic traffic rerouting to healthy servers
- Graceful degradation of non-critical features
- Priority queue for critical operations

Scenario 2: Complete Data Centre Failure

- Immediate failover to secondary region
- DNS update for traffic redirection
- Full service restoration within 2 hours

Scenario 3: Third-Party API Outage

- Cached data serving for read operations
- Queue write operations for later sync
- Alternative API endpoints activation

Scenario 4: Cyber Security Incident

- Immediate isolation of affected systems
- Activate clean backup infrastructure
- Forensic analysis in parallel

Crisis Management Activation

Activation Triggers:

- Service downtime exceeding 1 hour
- Data breach or security incident
- Natural disaster affecting operations
- Critical vendor/partner failure

Continuity Testing Schedule

Annually: Comprehensive compliance check and validation

Supplier & Vendor Continuity

- **PlanetScale:** 99.99% uptime SLA with automatic failover
- **Railway:** Multi-region deployment with instant scaling
- **Meta/TikTok/Google APIs:** Fallback mechanisms and cached operations
- **Payment Processors:** Multiple provider redundancy

23. Security Incident Response

Incident Response Protocol

1. **Detection:** Continuous monitoring for security threats and anomalies
2. **Assessment:** Immediate evaluation of incident severity and scope
3. **Containment:** Swift action to prevent further damage or data exposure
4. **Notification:** Affected users notified within 72 hours as required by law
5. **Recovery:** Restoration of services and data integrity
6. **Review:** Post-incident analysis and security improvements

24. Advanced Security Features

Active Protection

- Real-time threat detection
- DDoS protection
- Web Application Firewall (WAF)
- Rate limiting and API throttling
- Suspicious activity alerts

Monitoring & Logging

- Comprehensive audit logs
- Login history tracking
- API usage monitoring
- Campaign modification logs
- Spending alerts and limits

25. Product Security Features

Authentication Options

- **OAuth 2.0:** Supported for all platform integrations
- **Google SSO:** Single sign-on via Google accounts
- **Magic Links:** Passwordless authentication via email
- **MFA:** Multi-factor authentication available via Google OAuth (when users enable MFA on their Google account)
- **Hardware Keys:** YubiKey and other hardware security keys supported via Google account

Customer Audit Logs

- Audit logs available to customers
- Logs transmitted with TLS encryption
- Activity tracking for all user actions
- Campaign and ad modification history

Passwordless Security

AdManage.ai operates a passwordless authentication model for customers. Users authenticate via Google SSO, email magic links / OTP, or WorkOS SSO for eligible organisations, eliminating password-related vulnerabilities such as weak passwords, password reuse, and credential stuffing. MFA is available when enabled on the user's Google account or organisation IdP.

26. ESG & Ethics

Code of Ethics & Conduct

AdManage.ai maintains a Code of Ethics and Conduct that applies to all employees, contractors, and business partners.

- Commitment to integrity and ethical business practices
- Respect for privacy and data protection
- Fair treatment of all stakeholders
- Compliance with applicable laws and regulations
- Whistleblower protection for reporting concerns

27. Your Security Responsibilities

To maintain the security of your AdManage.ai account and advertising campaigns:

- **Keep your Google account secure** if using Google sign-in
- **Protect your email account** used for magic link authentication
- **Keep your connected ad accounts secure** on Meta, TikTok, and Google
- **Use only HTTPS URLs** for all landing pages and tracking links
- **Regularly review account activity** and report suspicious behaviour
- **Protect your API keys and tokens** - never share them publicly
- **Keep your browser and devices updated** with latest security patches

28. Security Contact

For security concerns, vulnerability reports, or questions about our security practices:

Security Team / Data Protection Officer: security@admanage.ai

General Support: support@admanage.ai

Priority Support: Available Monday-Friday, UK business hours for Enterprise customers

Responsible Disclosure: We appreciate security researchers who responsibly disclose vulnerabilities. Please email security@admanage.ai with details.

29. Policy Updates

This Security Policy may be updated periodically to reflect changes in our security practices, technology updates, or regulatory requirements. We will notify users of significant changes via email or platform notifications.

Last reviewed: 21 August 2026
Version: 2.0