GTA TECHNOLOGY, LLC

TERMS AND CONDITIONS
Last updated: March 18th, 2026

1. Overview and Contract Formation

These Terms and Conditions ("Terms") govern access to and use of the Protect by GTA client application (the "Client App"), the Protect Advisor by GTA application (the "Advisor App"), the Arti Assist application, and all related web portals, websites, and services (collectively, "Protect," "Arti Assist," or the "Services"). This includes all platforms and websites operated by GTA Technology, LLC, such as the Protect by GTA mobile app, the Protect Advisor by GTA mobile app, the Arti Assist application, the ProtectGTA.com web application, the ProtectGTA.com website, the Arti-Assist.com website, and the GTA-Technology.com website.

By creating an account, downloading either app, or using Protect, you agree to these Terms on behalf of yourself and any entity, family member, or delegate you authorize ("Authorized User"). If you do not agree, do not use Protect. Protect is a communication, workflow, and compliance platform that connects licensed insurance advisors and their clients. It is not an insurance agent, producer, or carrier and does not solicit, sell, or bind insurance policies or provide legal or tax advice. Protect does not collect or sell consumer data for marketing or advertising purposes.

2. Definitions

Advisor: Licensed insurance professional using Protect Advisor.
Client: Individual or business using Protect Client, invited by an Advisor.
Authorized User / Delegate: Family member, staff, accountant, attorney, or other individual granted access by a Client or Advisor.
AMS: Agency Management System used by an advisor or agency.
TruthSource™, RiskShield™, ProtectAI™, AssetLogic™, DataLift™, ProtectXtract™, GTAXtract™: Proprietary modules and engines developed by GTA Technology.
ACORD Forms / COIs: Industry-standard insurance forms referenced in connection with advisor workflows.

3. Scope of Service

Protect is a communication, data-management, and risk-identification platform that enhances collaboration between insurance advisors and their clients. It uses proprietary technology and AI to analyze information from the advisor's AMS, client inputs, and public or syndicated data to identify potential risks, inconsistencies, or missing information.

Protect streamlines information exchange, document sharing, and data validation, allowing advisors and clients to work together efficiently and accurately. Clients can request documents such as certificates of insurance (COIs), upload required information, and view centralized insurance data including policies, assets, ID cards, and inventories.

Protect does not issue, modify, or bind insurance coverage, nor does it generate or approve official insurance documents such as ACORD forms or COIs. Those documents are created, approved, and delivered by the licensed advisor through their AMS or carrier systems. Protect facilitates secure collaboration, information gathering, and delivery of finalized materials once approved by the advisor. Protect may also generate alerts, recommendations, Smart Reports, and risk insights from AMS data, client-entered data, public records, third-party data, or any combination of those sources, and such outputs may be made available to both the client and the advisor as part of the Services even where the underlying client-entered documents or records are not separately shared in full.

4. Licensing and Regulatory Responsibility

Protect is used by licensed insurance agencies and their authorized personnel. Access within Protect follows the agency's AMS configuration and internal permissions. GTA Technology does not verify or manage individual licensing status. Each agency is solely responsible for ensuring that all users of Protect under its account, including licensed producers, customer service representatives, and other staff, operate in accordance with applicable state and federal licensing, supervision, and compliance requirements.

5. Accounts, Invitations, and Roles

Clients may only join Protect through Advisor invitation. Advisors and Clients may invite delegates; each Authorized User must register individually and is bound by these Terms. Access is role-based.

Advisor and broker personnel access to a particular client relationship within Protect depends on the applicable AMS security profile and related advisor-client relationship. If

an advisor or broker does not have access to a client relationship through the AMS security profile, that individual will not have access to that client's information in Protect.

Delegates and other Authorized Users may access only the information and functions specifically made available to them by the inviting account holder or applicable platform permissions. Delegates do not receive access to AMS-derived data unless otherwise permitted through the applicable advisor-client relationship and system authorization. Actions by Authorized Users are attributable to the inviting account holder or the account through which such access was granted.

6. SMS Authentication and Security Verification

Protect may send one-time password (OTP) authentication codes to the mobile phone number associated with your account to verify your identity and protect account access.

By providing your mobile phone number within the Protect platform, you consent to receive SMS messages used solely for login authentication and account security.

Message frequency depends on login activity or verification requests. Standard carrier message and data rates may apply.

You may opt out by replying **STOP** to any authentication message. Reply **HELP** for assistance. Please note that opting out may prevent you from accessing **your account or certain features that require SMS verification**.

Protect uses mobile numbers only for authentication and security purposes and does **not use or share mobile numbers for marketing or promotional communications**.

For questions regarding SMS communications, contact: **privacy@gta-technology.com**

7. Data Collection and Use

Protect may collect, process, or store Identity Data, Insurance Data, Business & Asset Data (including asset inventories, receipts, attachments, and photographs for recordkeeping and validation), Client-Uploaded Documents, Claims Data, Syndicated & Public Data (for example ATTOM, NOAA, FEMA), and Derived Data.

If a government-issued ID or other sensitive document is uploaded, including a driver's license, passport, tax document, legal record, or similar file, Protect may securely store

that document to enable cross-device access, recordkeeping, and controlled sharing within the platform.

Protect does not modify, redact, or alter user-uploaded documents. Documents are stored as provided by the user and are accessible only in accordance with AMS-based authorization, platform role controls, and user-configured sharing settings as described in these Terms.

Users are responsible for determining what information they choose to upload, store, enter, and share within the platform, including any sensitive personal, financial, legal, business, or insurance-related information. Users are also responsible for managing sharing settings and access permissions and should carefully consider what information is shared and with whom.

Protect may use uploaded or user-entered information to classify documents, organize records, generate alerts, and create recommendations, Smart Reports, risk insights, or other service outputs. Such outputs may be made available to both the client and the advisor as part of the Services, even where the underlying client-entered documents or records are not separately shared in full, and without exposing the full contents of such documents except as otherwise authorized by the user.

Protect is designed to limit unnecessary exposure of highly sensitive identifiers, such as full government ID numbers or full Social Security numbers, in ordinary service outputs where they are not required.

Protect connects directly to the advisor's AMS and imports client, policy, and related operational data needed to provide the Services. It also connects to carrier portals and document systems where available and uses public and syndicated data to enrich records and identify risk.

Protect uses multiple categories of data within the Services. Some information is imported from the AMS or other connected systems and is governed by those authorization models. Other information is entered or uploaded directly by the client and remains subject to client-controlled sharing settings. Protect may also generate alerts, reports, recommendations, Smart Reports, and risk insights based on AMS data, client-entered data, public records, third-party data, or any combination of those inputs. System-generated outputs, including alerts, recommendations, Smart Reports, and risk insights, are part of the core functionality of the Services and are not subject to user-controlled sharing settings applicable to underlying client-entered documents.

Protect uses data to operate the platform, reconcile and validate information, enrich profiles, identify risks, support claims communication, generate Smart Reports, recommendations, and risk insights, and provide clients with recordkeeping and inventory tools. Protect uses administrative, technical, and physical safeguards designed to protect information handled through the Services, including encryption in transit and at rest, permission-based access controls, role-based restrictions, authentication controls, audit logging, and AWS-hosted enterprise-grade infrastructure.

Protect complies with GLBA. Records are retained for seven (7) years; only legally required data is retained after termination. Records are retained not only for compliance but also to support discovery and legal defense in lawsuits or disputes. These records serve as neutral evidence intended to protect both advisors and clients by maintaining an immutable history of actions and communications.

8. GLBA and Privacy Compliance

Protect acts solely as a service provider between Advisors and Clients. It complies with the GLBA Safeguards Rule and does not sell or license nonpublic personal information. Agencies and Advisors are responsible for any legally required consents, notices, supervisory controls, and compliance obligations arising from their advisor-client relationships, licensing status, or AMS data practices.

9. Children's Access

Protect is not designed for children under 18. Users must be 18 or older to register directly. A Client or Advisor may invite individuals aged 16 or 17 who are insured under an active policy, provided the invitation is issued by a parent, guardian, or Advisor. Such access is limited to necessary insurance functions such as viewing ID cards or contributing to inventories. Protect is not intended for users under 16.

10. Payments and Subscriptions

Client App: Free download; subscription required. Advisor App: Free download; requires onboarding. Annual plans are paid in advance, non-refundable, and end at term. Monthly plans end at the last paid month, non-refundable. Accounts may be suspended for nonpayment.

User-provided data is retained for 30 days after suspension and then deleted permanently except for legally required records. If the account is reactivated, AMS data will repopulate

automatically but uploaded data will not be recoverable. Protect may suspend or terminate accounts for excessive chargebacks.

11. Intellectual Property and Proprietary Rights

Protect and all related software, interfaces, data structures, algorithms, and processing logic are the exclusive property of GTA Technology, LLC and are protected by United States and international copyright, patent, and trade-secret laws.

The Protect platform and its proprietary modules (TruthSource™, RiskShield™, ProtectAI™, AssetLogic™, DataLift™, ProtectXtract™, GTAXtract™) contain patent-pending processes, copyrighted code, and proprietary technology developed exclusively by GTA Technology, LLC. This includes the Protect AI Engine, proprietary data-mapping methods, compliance logic, and workflow automation models that embody trade secrets and confidential business information.

Users receive a limited, revocable license to access the Services during an active subscription. Any attempt to copy, reverse engineer, decompile, resell, or replicate any part of Protect's technology, design, or data model is strictly prohibited and will be pursued to the fullest extent of the law. All enhancements, derivatives, and feedback related to Protect become the sole property of GTA Technology, LLC. Unauthorized use of Protect's proprietary systems, AI models, or compliance framework may result in civil and criminal liability under applicable laws.

12. AI and Automated Processing

Protect uses proprietary AI and vetted large language models to support automation, validation, document handling, organization, risk identification, and compliance-related workflows.

AI may transform, summarize, classify, organize, validate, and analyze text, documents, and records to deliver and improve the Services, support document handling, identify issues, and generate alerts, recommendations, Smart Reports, and risk insights. AI and related automated processes may also be used to help identify and limit unnecessary exposure of highly sensitive identifiers in ordinary service outputs where such identifiers are not required.

Protect's AI continuously reviews publicly available and licensed regulatory data from local, state, federal, and carrier sources to identify new risks or compliance requirements.

AI systems may also prioritize and present risk insights in plain language for advisors and clients.

All AI-generated outputs are informational only and require Advisor review before use in client or business decisions.

13. User Responsibilities

Users must provide accurate information, maintain credential and device security, review outputs before use, and manage sharing settings and delegate access responsibly.

Advisor and broker access to AMS-derived information is governed by the AMS security profile and related advisor-client relationship. Client-entered information shared within Protect is subject to additional client-controlled permissions within the platform.

Users are responsible for determining what information they upload, store, enter, and share within the platform, including any sensitive personal, financial, legal, business, or insurance-related information.

Users are also responsible for managing access permissions for delegates and for any client-entered information they choose to make available through Protect. Once access is granted to any advisor, delegate, or third party, GTA Technology does not control how such information is further used, retained, or shared by that party.

13A. Sensitive Information and User-Controlled Sharing

Protect may be used to store sensitive personal, financial, legal, business, and insurance-related documents and information.

Users are responsible for determining what information they upload, store, enter, and share within the platform and for managing sharing settings and access permissions for delegates and other authorized users.

Protect does not verify the identity, authority, or legal status of any delegate or other person granted access by the user and is not responsible for how information is used once access has been granted by the account owner or other authorized user.

14. Acceptable Use

Users may not reverse engineer or copy Protect, train external AI models on its outputs, upload unlawful or infringing content, or attempt to circumvent security controls. Users may not use the Services to grant access to information in violation of applicable law, contractual obligations, fiduciary duties, or court-imposed restrictions.

15. Feedback

Any ideas, feedback, or suggestions submitted to GTA Technology become the property of GTA Technology, LLC without restriction or obligation.

16. Legal Terms

Governing Law. These Terms are governed by the laws of the State of Florida, excluding its conflict-of-law principles, and any arbitration or litigation shall occur in **Collier County, Florida**.

Dispute Resolution. Disputes shall be resolved by confidential binding arbitration under **AAA** or **JAMS** rules in Collier County, Florida. Users waive the right to class actions or jury trials.

Limitation of Liability. GTA Technology's total liability shall not exceed the greater of fees paid in the previous 12 months or $25,000. Neither party is liable for indirect, consequential, incidental, special, exemplary, or punitive damages, including loss of profits, loss of goodwill, loss of data, or business interruption, even if advised of the possibility of such damages. GTA Technology is not liable for unauthorized access, disclosure, or use of information resulting from user actions, sharing decisions, compromised credentials, third-party misuse after authorized access has been granted, or circumstances outside GTA Technology's reasonable control. GTA Technology is not responsible for any decisions, actions, or omissions taken by advisors, clients, delegates, or other users based on information, alerts, recommendations, Smart Reports, or risk insights provided through the Services.

Indemnification. Users indemnify, defend, and hold harmless GTA Technology from claims, losses, liabilities, damages, and expenses arising from misuse of the Services, inaccurate or unlawful content, unauthorized sharing, violation of these Terms, or access granted by the user to delegates, advisors, or other third parties. GTA Technology

indemnifies users for claims that the Protect platform infringes third-party intellectual property rights, subject to customary exclusions.

Trade Controls. Protect may not be used in sanctioned countries.

17. Termination

Protect may suspend or terminate accounts for breach, unlawful use, nonpayment, or chargebacks. Upon termination, access ceases and user-provided data is deleted as described in the applicable retention and deletion provisions. AMS-derived data may repopulate upon reactivation where available, but deleted uploaded or client-entered data may not be recoverable.

18. Notices

GTA Technology, LLC
365 5th Ave. S, Suite 201
Naples, Florida 34102
Email: **privacy@gta-technology.com**

19. Entire Agreement

These Terms, together with any subscription agreement, data-processing addendum, or master services agreement, constitute the entire agreement between you and GTA Technology, LLC regarding Protect.