Markdale Financial Management – Privacy Policy

Effective Date: May 2026

Last Updated: May 2026

1. Introduction & Scope of the Policy

At Markdale Financial Management ("Markdale", "we", "us", or "our"), safeguarding the confidentiality, privacy, and security of our clients' financial and personal information is one of our highest priorities. As part of work, we are committed to maintaining robust privacy standards that protect your data while leveraging modern technology to deliver premium wealth management services.

This Privacy Policy herein governs the collection, usage, storage, and protection of data belonging to our current, past, and prospective clients, as well as workflows managed by Markdale staff.

2. Information We Collect

To provide documentation, reporting, tax preparation, and other financial services, we collect several categories of information, including:

- **Personal Identifiers:** Names, physical addresses, email addresses, and phone numbers.
- **Government Identifiers:** Social Insurance Numbers (SIN) or other national tax identification numbers.
- **Financial Data:** Asset details, net worth statements, investment histories, bank account details, and risk tolerance profiles.
- **Transactional & Operational Data:** Account statements, transaction histories, and portfolio performance metrics.

3. Why We Collect, Use, and Disclose Information

Markdale collects, uses, and discloses personal, financial, and operational information only for purposes reasonably connected to providing family office, administrative, reporting, bookkeeping, investment-policy, coordination, and related services to our clients.

These purposes include:

- Onboarding new clients and establishing client records.
- Verifying client identity and contact information.
- Maintaining accurate records of family members, entities, trusts, corporations, foundations, advisors, and authorized representatives.
- Preparing consolidated financial, investment, bookkeeping, and administrative reports.
- Maintaining records of assets, liabilities, transactions, account statements, cost information, income, expenses, tax-related data, and supporting documents.

- Coordinating with accountants, lawyers, investment advisors, private bankers, custodians, trustees, insurance professionals, and other client-authorized representatives.
- Supporting tax preparation, audit requests, estate planning, philanthropic planning, investment policy documentation, and other client-directed projects.
- Administering invoices, payments, accounts receivable, accounts payable, and firm accounting.
- Monitoring data quality, reconciling information, identifying discrepancies, and improving internal workflows.
- Maintaining appropriate access controls, cybersecurity protections, audit trails, and operational safeguards.
- Complying with legal, tax, regulatory, audit, contractual, and professional obligations.
- Responding to client inquiries, instructions, complaints, or requests.
- Protecting the rights, property, confidentiality, and security of Markdale, our clients, and authorized third parties.

Markdale does not sell, rent, or trade client personal information. We only disclose information where reasonably necessary to provide services, where authorized by the client, where required by law, or where otherwise permitted by applicable privacy legislation.

4. Storage Infrastructure & Access Architecture

Markdale utilizes **Google Drive** as our primary cloud storage and secure document collaboration environment. Access to this environment is managed using administrative and technical controls designed to protect the confidentiality, integrity, and availability of client records.

4.1 Authorized Ecosystem Users & Verification Requirements

To facilitate collaborative, multi-family wealth management, access to specific segments of our Google Drive environment may be extended to external parties. However, access is never granted automatically and is strictly subject to verification protocols:

- **Markdale Internal Staff:** Authorized personnel requiring access to perform daily administrative, operational, compliance, and advisory functions.
- **Authorized Family Members:** Immediate or designated family members of the client. Access is granted strictly upon receiving explicit client authorization via a signed written agreement or verified email confirmation.
- **Authorized Professional Advisors:** External third-party professionals acting on the client's behalf, including external investment advisors, private bankers, legal counsel (lawyers), and accountants.
- **Mandatory Confidentiality Bounds:** Before any external professional advisor or representative is granted access to a folder, Markdale requires documented client confirmation. Furthermore, these representatives must be bound either by established

professional codes of confidentiality (e.g., legal or CPA ethics) or an explicit written non-disclosure agreement.

4.2 "Need-to-Know" Access Control & Governance

- **Restricted Permissions:** Access to our Google Drive is governed strictly by a **"need-to-know" framework** rather than broad, firm-wide, or portfolio-wide permissions. External third parties, professional advisors, and family members are strictly restricted from broad system access and are only granted targeted visibility into the specific files and folders directly relevant to their specialized scope of work.
- **Access Governance:** Management and administrative authority over folder permissions rests exclusively with the designated **owners** of the respective Google Drive folders, who are comprised of select, authorized staff members of Markdale. These folder owners are responsible for provisioning, auditing, and promptly revoking access permissions to ensure data security.

4.3 Client-Directed Storage Alternatives

While Markdale utilizes Google Drive as its default secure environment, we recognize that certain clients or family offices prefer alternative architectures. Clients may elect to host their financial records within a private cloud environment of their choosing (e.g., a client-owned Microsoft SharePoint, Box Enterprise, or alternative secure drive). Where a client selects a custom storage alternative, Markdale will adapt its workflows to interface directly with the client-managed environment, subject to verifying that the environment meets our technical security standards.

5. Financial Platform & Core Technology Integrations

In addition to our storage infrastructure, Markdale securely integrates client data with specialized, market-leading financial technology and accounting platforms to perform operational and reporting functions. These platforms include, but are not limited to:

- **Addepar:** Utilized as our core wealth management platform for portfolio performance tracking, asset aggregation, data consolidation, and client wealth reporting. Selected transactional data and account statement metrics are securely synced to Addepar to provide clients with accurate portfolio insights.
- **QuickBooks Online:** Utilized for firm billing, invoicing, corporate accounting, and financial record-keeping. Relevant billing and high-level client financial data required for transactional processing are managed within this secure environment.
- **Access Restraints:** Data shared with these platforms remains fully protected under our firm's overarching "need-to-know" access rules. Access permissions within Addepar and QuickBooks Online are tightly restricted to select Markdale operational staff and client representatives.

6. Safeguards and Security Measures

Markdale uses administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, use, disclosure, alteration, loss, or destruction. The level of protection applied depends on the sensitivity of the information, the volume involved, the nature of the client relationship, and the operational purpose for which the information is used.

- **Multi-Factor Authentication (MFA):** Markdale uses multi-factor authentication where appropriate to help protect access to cloud-based systems, document repositories, financial platforms, email accounts, and other sensitive business systems. MFA reduces the risk that a compromised password alone could allow unauthorized access to client information.
- **Role-Based and Need-to-Know Access:** Access to client information is restricted based on role, responsibility, and operational need. Markdale personnel, contractors, family members, professional advisors, and other authorized representatives are only granted access to information reasonably necessary for their specific function or mandate. External parties are limited to specific folders, files, reports, or records relevant to the client-authorized purpose.
- **Password Management:** Markdale requires passwords and credentials to be handled securely. Personnel are expected to use strong, unique passwords for business systems and to avoid sharing credentials. Where appropriate, Markdale uses password-management tools and administrative controls to support secure credential storage, access, and revocation.
- **Access Reviews and Permission Management:** Markdale periodically reviews access permissions for key systems and document repositories. Access may be modified or revoked when a person's role changes, when an engagement ends, when a client withdraws authorization, or when access is no longer required.
- **Offboarding Procedures:** When an employee, contractor, advisor, representative, or other authorized user no longer requires access to client information, Markdale takes reasonable steps to revoke or modify access in a timely manner. This includes disabling accounts, removing Google Drive or platform permissions, changing shared credentials where applicable, recovering firm property, and confirming that access to sensitive systems has been terminated.
- **Staff Training and Confidentiality:** Markdale personnel are expected to understand and comply with privacy, confidentiality, data-handling, and cybersecurity expectations. Staff training and internal guidance address secure document handling, phishing awareness, appropriate use of client information, secure sharing practices, AI-related safeguards, incident escalation, and the importance of maintaining client confidentiality.
- **Incident Response Escalation:** Markdale maintains internal procedures for escalating and responding to suspected privacy or security incidents. Personnel are expected to promptly report suspected unauthorized access, accidental disclosure, lost devices,

phishing events, unusual system activity, or other concerns that may affect the confidentiality, integrity, or availability of client information.

7. Deployment of Artificial Intelligence (AI) Technologies

Markdale may use AI tools to support selected internal administrative, document-processing, reconciliation, coding, summarization, and quality-control workflows. When utilizing advanced Artificial Intelligence (AI) platforms, including Google Gemini, OpenAI ChatGPT, and Anthropic Claude, our deployment is governed by data minimization boundaries and institutional-grade protections.

7.1 Permitted Use of AI Tools & Precise Operational Scope

AI technologies are utilized strictly as internal administrative and workflow-enhancement utilities. Our precise operational scope includes:

- **Data Validation & Quality Assurance:** Employing AI to audit, cross-reference, and validate financial reporting metrics to reduce human calculation errors.
- **Anomaly Detection & Reconciliation:** Utilizing AI to identify discrepancies, irregular patterns, or reconciliation mismatches across transactional logs.
- **Classification & Extraction:** Deploying AI scripts to write, debug, and execute code used to read PDF account statements, classify document types, and extract unstructured table data into organized, searchable datasets.
- **Consolidation & Report Generation:** Summarizing long-form financial research, market commentary, meeting transcripts, and internal metrics to draft preliminary administrative reports and insights.

7.2 Strict Data Minimization Boundaries & Guardrails

To protect core client identities, we enforce strict segregation between highly sensitive legal documentation and our integrated AI workflows.

- **Connected Environments:** Markdale securely connects specific, isolated folders within our corporate Google Drive to our AI tools to facilitate automated data organization.
- **Permitted Folder Contents:** These designated folders may contain institutional or individual **account statements**, which include client names, corporate entity names, physical addresses, and account numbers. This data is required for the AI to accurately validate reporting and parse statements.
- **Prohibited Data (The Exclusion Rule):** Markdale's policy is not to upload account-opening documentation, Social Insurance Numbers, or tax documents to AI platforms, unless specifically authorized, legally required, or approved under a documented exception process. These files remain isolated in segregated, non-AI-integrated cloud repositories.

7.3 Governance, Model Training Opt-Out, and Human Review Limits

Our deployment of AI tools is governed by corporate service frameworks designed to limit third-party vendor visibility:

- **Contractual Protections:** Where available, Markdale uses business-grade or enterprise-grade service arrangements, administrative settings, and contractual protections designed to limit vendor use of client information and support appropriate data protection, confidentiality, and security.
- **Model Training Prohibitions:** Where available, Markdale uses business, enterprise, or API-based AI services with settings or contractual terms designed to prevent client content from being used to train public AI models. Markdale periodically reviews vendor terms, administrative settings, and internal practices as these services evolve.
- **Vendor Human Review Restrictions:** Markdale configures AI tools, where available, to reduce or prevent vendor human review of client content, subject to applicable service terms, security requirements, legal obligations, and exceptional support or abuse-prevention processes.
- **Absolute Protection of AI Outputs:** Any outputs, insights, structured sheets, or synthesized documents *derived* from AI processing are treated as Confidential Information. They remain subject to the exact same stringent security protocols, encryption parameters, and confidentiality obligations as the original source inputs.

7.4 No Automated Decision-Making

Markdale does not use AI tools to make automated investment, legal, tax, credit, eligibility, or fiduciary decisions about clients. AI outputs are treated as drafts, tools, or inputs only and are subject to human review before being used in client deliverables, reporting, bookkeeping, or decision-making.

7.5 Client Opt-Out and Processing Preferences

Markdale firmly believes in client data autonomy. The AI-driven data validation, reconciliation, and summarization workflows outlined in this section represent our standard operational efficiency model. However, these workflows are entirely modular. Clients have the absolute right to opt out of AI-assisted processing. If an opt-out is exercised, Markdale will process, validate, and reconcile all client reporting and statements utilizing traditional, manual human workflows exclusively.

8. Retention and Destruction of Information

Markdale retains personal information only for as long as reasonably necessary to fulfill the purposes for which it was collected, to provide services to clients, to maintain accurate business and financial records, and to satisfy legal, tax, regulatory, audit, contractual, insurance, and professional obligations.

Retention periods may vary depending on the nature of the information, the client relationship, the type of record, applicable legal requirements, and operational needs. For example, certain financial, tax, corporate, trust, estate, bookkeeping, investment, and audit-related records may need to be retained for extended periods.

When personal information is no longer required, Markdale will take reasonable steps to securely delete, destroy, anonymize, or archive the information in accordance with our internal record-retention practices and applicable legal requirements. Secure destruction may include deletion from cloud-based systems, removal of access permissions, destruction of paper records, or other commercially reasonable disposal methods.

Where information has been shared with authorized third-party service providers, Markdale will rely on contractual, technical, and administrative safeguards designed to ensure that such providers retain and dispose of information appropriately.

9. Privacy Breach Notification and Incident Response

Markdale maintains procedures to identify, assess, contain, investigate, and respond to suspected or actual privacy and security incidents involving personal information under our control.

If Markdale becomes aware of a privacy or security incident, we will take reasonable steps to:

- Contain the incident and prevent further unauthorized access, use, or disclosure.
- Assess the nature and sensitivity of the information involved.
- Determine the cause and scope of the incident.
- Evaluate whether the incident creates a real risk of significant harm to affected individuals.
- Notify affected individuals, regulators, service providers, insurers, professional advisors, or other parties where required or appropriate.
- Document the incident and Markdale's response.
- Implement remedial measures designed to reduce the risk of recurrence.

Where required by applicable law, Markdale will provide breach notifications to affected individuals and applicable privacy regulators. Notifications may include a description of the incident, the type of information involved, steps taken by Markdale, steps individuals may wish to take to protect themselves, and contact information for further questions.

10. Client Rights and Policy Updates

You maintain the right to review the personal information Markdale holds on your behalf and request corrections to any inaccuracies.

Before responding to an access or correction request, Markdale may take reasonable steps to verify the identity and authority of the person making the request. In some cases, access to information may be limited by legal, regulatory, confidentiality, privilege, security, or third-party privacy considerations.

We review this policy continuously to align with evolving regulatory frameworks and technological deployments. Material changes regarding how we handle data will be communicated directly to clients via our secure client portal or direct electronic communication.

11. Privacy Contact / Contact Us

Markdale is responsible for personal information under its control and has designated a privacy contact responsible for overseeing our privacy practices, responding to privacy-related questions, and coordinating access, correction, and complaint requests.

Questions about this Privacy Policy, Markdale's privacy practices, or requests to access or correct personal information may be directed to:

Markdale Financial Management Attention: James Dunne

Email: james@markdalemanagement.com

Phone: 416-602-9209

Schedule A: Client Privacy & Data Governance Preferences

Client Name(s): _____

Date: _____

Please review the choices below to customize how Markdale Financial Management stores your data and utilizes operational efficiency tools during our business relationship. These selections can be modified at any time.

Part I: Document Storage & Collaboration Infrastructure

Please select where you would prefer Markdale to maintain, organize, and collaborate on your family office documents, financial statements, and corporate records:

- [ ] **Option A: Markdale-Managed Google Drive (Default)** *I authorize Markdale to utilize its secure Google Drive environment, subject to the strict role-based and "need-to-know" access restrictions detailed in Section 4 of the Privacy Policy.*
- [ ] **Option B: Client-Managed Secure Drive** *I prefer to host all of our family/corporate documentation within our own secure data repository. Markdale staff will be granted restricted access to our external environment, and no core documents will be duplicated into Markdale's default Google Drive. Please specify platform (e.g., SharePoint, Box, Citrix ShareFile):* _____

Part II: Artificial Intelligence (AI) Workflow Preferences

Markdale utilizes enterprise-contracted AI environments (Google Gemini, OpenAI ChatGPT, Anthropic Claude) with settings and contractual terms designed to limit data usage and restrict vendor human review to automate document parsing, validate reporting data, and detect transactional anomalies.

Please select your processing preference:

- [ ] **Option A: Full Workflow Optimization (Opt-In)** *I authorize Markdale to utilize secure AI tools to validate reporting, parse statement tables, and summarize research or meeting logs containing our account data (excluding SINs and Tax Documents), as outlined in Section 7 of the Privacy Policy.*
- [ ] **Option B: Restricted AI Processing (Selective Validation Only)** *I authorize Markdale to use AI tools strictly for internal administrative scripts, coding, and document summarization, but* ***prohibit*** *the system from reading or processing our specific account statements or transactional logs.*
- [ ] **Option C: Total AI Opt-Out (Manual Workflows Only)** *I explicitly* ***opt out*** *of all AI-assisted processing workflows. I request that all data validation, report cross-referencing, document summarization, and table extraction related to our accounts be performed exclusively by manual human review.*

Part III: Acknowledgement & Authorization

By signing below, I confirm that I have reviewed the Markdale Privacy Policy and that the choices selected above accurately reflect my data governance preferences.

Client Signature: _____ **Date:** _____

Co-Client Signature: _____ **Date:** _____