COMPLIANCE POLICY MANUAL
Document Retention & Information Security

Version 4.2 | Effective Date: January 1, 2026 | Approved by: Managing Partners Committee
Classification: CONFIDENTIAL — Internal Use Only

TABLE OF CONTENTS

PART I — DOCUMENT RETENTION POLICY

Section 1. PURPOSE AND SCOPE

1.1 Purpose. This Document Retention Policy ("Policy") establishes the requirements for the retention, management, and destruction of all documents and records created, received, or maintained by Hargrove & Associates LLP (the "Firm") in the course of its business operations and legal practice.

1.2 Scope. This Policy applies to all partners, associates, of counsel, paralegals, staff, contractors, and any other individuals who create, access, or manage Firm records, regardless of format (paper, electronic, audio, video, or other media).

1.3 Legal Basis. This Policy is designed to comply with applicable federal and state laws, regulations, and professional obligations, including: (a) the Sarbanes-Oxley Act; (b) the Federal Rules of Civil Procedure; (c) IRS record retention requirements; (d) state bar ethics rules governing attorney record-keeping; and (e) SEC Rule 17a-4 (where applicable to regulated clients).

1.4 Definitions. "Document" or "Record" means any recorded information, regardless of form or characteristics, including correspondence, memoranda, contracts, reports, emails, instant messages, spreadsheets, databases, voicemails, photographs, and metadata.

Section 2. RETENTION SCHEDULE

2.1 General Retention Periods. The following minimum retention periods shall apply:

Document Category	Retention Period
Client engagement letters	Permanent
Client matter files (active)	Duration of engagement + 7 years
Client matter files (closed)	10 years from matter closing
Privileged communications	Permanent (unless waived)
Corporate formation documents	Permanent
Financial records and tax returns	7 years
Employee personnel records	7 years after termination
Contracts and agreements	10 years after expiration
Billing records and invoices	7 years
Trust account records (IOTA)	7 years
Marketing materials	3 years
General correspondence	5 years
Internal memoranda	5 years
Board/partner meeting minutes	Permanent
Insurance policies	Permanent
Real estate records	Permanent
Litigation files	10 years after final disposition
Regulatory filings	Permanent

2.2 Electronic Records. Electronic records are subject to the same retention periods as their paper equivalents. Email messages that constitute substantive business records must be preserved in accordance with this schedule.

2.3 Exceptions. The Chief Compliance Officer may authorize exceptions to the retention schedule for specific categories of records upon written request and with documented justification.

Section 3. ELECTRONIC RECORDS MANAGEMENT

3.1 Document Management System. All Firm documents shall be stored in the Firm's approved document management system (currently iManage Work). Documents stored outside the DMS are not subject to the Firm's backup and disaster recovery protections and may be subject to disciplinary action.

3.2 Naming Conventions. All electronic documents shall follow the Firm's naming convention: [ClientNo]-[MatterNo]-[DocType]-[Description]-[YYYY-MM-DD].

3.3 Email Management. Emails related to client matters must be filed in the appropriate matter folder within the DMS within five (5) business days of receipt or sending. Personal emails must not be stored in client matter folders.

3.4 Cloud Storage. Use of personal cloud storage services (Dropbox, Google Drive, iCloud, etc.) for Firm or client documents is strictly prohibited. Only Firm-approved cloud services with appropriate security controls may be used.

3.5 Mobile Devices. Client documents may be accessed on mobile devices only through Firm-approved secure applications with remote wipe capability.

Section 4. LEGAL HOLDS

4.1 Obligation to Preserve. When litigation is reasonably anticipated, pending, or ongoing, the Firm has a legal obligation to preserve all documents that may be relevant to the matter. The Chief Compliance Officer shall issue a written legal hold notice ("Legal Hold") to all custodians who may possess relevant documents.

4.2 Scope of Legal Hold. A Legal Hold supersedes all retention schedules and destruction authorizations. No documents subject to a Legal Hold may be destroyed, deleted, modified, or transferred without the express written consent of the Chief Compliance Officer.

4.3 Employee Obligations. Upon receiving a Legal Hold notice, each recipient must: (a) immediately cease any destruction of potentially relevant documents; (b) identify and segregate all responsive documents; (c) confirm receipt and compliance in writing within forty-eight (48) hours; and (d) continue to preserve documents until the Legal Hold is formally released.

4.4 Penalties. Failure to comply with a Legal Hold may result in disciplinary action, up to and including termination, and may expose the Firm to sanctions, adverse inference instructions, or other legal penalties.

Section 5. DESTRUCTION PROCEDURES

5.1 Authorized Destruction. Documents that have reached the end of their retention period and are not subject to any Legal Hold may be destroyed in accordance with this Section.

5.2 Destruction Methods. The following destruction methods are authorized:

Paper documents: Cross-cut shredding (DIN Level P-4 or higher)

Electronic media: NIST SP 800-88 compliant data sanitization

Hard drives: Physical destruction or degaussing
Optical media: Physical shredding

5.3 Destruction Certificate. A written certificate of destruction must be prepared for each destruction event, documenting: (a) the date of destruction; (b) a description of the documents destroyed; (c) the method of destruction; (d) the identity of the person supervising destruction; and (e) confirmation that no Legal Hold applies.

5.4 Third-Party Destruction. If destruction is performed by a third-party vendor, the vendor must execute a confidentiality agreement and provide a certificate of destruction.

PART II — INFORMATION SECURITY POLICY

Section 6. ACCESS CONTROLS

6.1 Principle of Least Privilege. Access to Firm systems and data shall be granted on a need-to-know basis, limited to the minimum level of access required to perform job functions.

6.2 Authentication Requirements. All users must authenticate using multi-factor authentication (MFA) consisting of: (a) a unique username and strong password (minimum 14 characters, including uppercase, lowercase, numbers, and special characters); and (b) a second factor using a hardware security key (YubiKey) or approved authenticator application.

6.3 Password Management. Passwords must be changed every ninety (90) days. Password reuse is prohibited for the previous twelve (12) passwords. Passwords must not be shared, written down, or stored in unencrypted form.

6.4 Remote Access. Remote access to Firm systems is permitted only through the Firm's virtual private network (VPN) with split tunneling disabled. Remote desktop protocol (RDP) access from outside the VPN is prohibited.

6.5 Privileged Accounts. Administrative and privileged accounts must be: (a) inventoried and reviewed quarterly; (b) subject to enhanced monitoring; (c) never used for routine tasks; and (d) protected by hardware MFA tokens.

Section 7. DATA CLASSIFICATION

7.1 Classification Levels. All Firm data shall be classified according to the following levels:

Level 1 — RESTRICTED: Attorney-client privileged communications, trade secrets, regulatory examination reports, client financial data, PII/PHI. Access limited to specifically authorized individuals.

Level 2 — CONFIDENTIAL: Client matter files, internal legal analyses, Firm financial records, personnel records, strategic plans. Access limited to Firm personnel with a business need.

Level 3 — INTERNAL: Internal policies, procedures, training materials, general correspondence. Available to all Firm personnel.

Level 4 — PUBLIC: Marketing materials, published articles, website content, press releases. No access restrictions.

7.2 Labeling. All documents classified as RESTRICTED or CONFIDENTIAL must bear the appropriate classification label in the header or footer.

7.3 Handling Requirements. Each classification level has specific handling requirements for storage, transmission, printing, and destruction as detailed in Appendix A.

Section 8. INCIDENT RESPONSE

8.1 Incident Response Team. The Firm maintains an Incident Response Team ("IRT") consisting of: (a) Chief Information Security Officer (Lead); (b) Chief Compliance Officer; (c) Managing Partner representative; (d) IT Director; and (e) outside cybersecurity counsel.

8.2 Incident Classification. Security incidents are classified as follows:

Critical: Active data breach involving client data or privileged information

High: Ransomware, advanced persistent threat, or unauthorized system access

Medium: Malware infection, phishing compromise, or policy violation

Low: Suspicious activity, failed intrusion attempts, minor policy deviations

8.3 Reporting. All personnel must report suspected security incidents to the IT Security team immediately upon discovery. The IRT shall be activated within one (1) hour for Critical and High incidents.

8.4 Notification. In the event of a data breach involving client data, the Firm shall notify affected clients within seventy-two (72) hours of confirmation of the breach, and shall comply with all applicable state breach notification laws.

8.5 Post-Incident Review. Following any Critical or High incident, the IRT shall conduct a post-incident review within thirty (30) days and document lessons learned, remediation actions, and preventive measures.

Section 9. THIRD-PARTY SECURITY

9.1 Vendor Assessment. Before engaging any third-party vendor that will access Firm systems or data, the IT Security team must complete a vendor security assessment covering: (a) SOC 2 Type II or equivalent certification; (b) encryption standards; (c) access controls; (d) incident response capabilities; and (e) data residency requirements.

9.2 Contractual Requirements. All vendor agreements must include: (a) confidentiality and data protection obligations; (b) breach notification requirements (within twenty-four (24) hours); (c) audit rights; (d) data return and deletion provisions; and (e) compliance with applicable laws.

9.3 Ongoing Monitoring. Third-party vendors with access to Level 1 or Level 2 data must be reassessed annually.

Section 10. EMPLOYEE OBLIGATIONS AND CONFIDENTIALITY

10.1 Acceptable Use. Firm computing resources are provided for business purposes. Limited personal use is permitted provided it does not: (a) interfere with job performance; (b) violate any Firm policy; (c) consume excessive bandwidth; or (d) expose the Firm to legal liability.

10.2 Prohibited Activities. The following are strictly prohibited: (a) unauthorized access to systems or data; (b) installation of unauthorized software; (c) use of personal email for Firm business; (d) connecting unauthorized devices to the Firm network; (e) disabling security software; (f) sharing login credentials; and (g) circumventing access controls.

10.3 Clean Desk Policy. All RESTRICTED and CONFIDENTIAL documents must be secured when unattended. Workstations must be locked when leaving the desk. Printing of RESTRICTED documents requires secure print release at the printer.

10.4 Confidentiality Obligations. All personnel must maintain the confidentiality of client information, Firm proprietary information, and any information designated as confidential. These obligations continue after separation from the Firm.

PART III — ENFORCEMENT AND COMPLIANCE

Section 11. TRAINING REQUIREMENTS

11.1 Initial Training. All new personnel must complete the following training within thirty (30) days of hire: (a) Information Security Awareness (2 hours); (b) Document Retention and Records Management (1 hour); (c) Phishing Awareness and Social Engineering (1 hour); and (d) Ethics and Professional Responsibility (1 hour).

11.2 Annual Refresher. All personnel must complete annual refresher training covering updated policies, emerging threats, and lessons learned from recent incidents.

11.3 Specialized Training. Personnel in elevated-risk roles (IT administrators, compliance officers, partners handling regulatory matters) must complete additional role-specific training as determined by the Chief Compliance Officer.

11.4 Training Records. All training completion records shall be maintained by the Human Resources department for the duration of employment plus seven (7) years.

Section 12. MONITORING AND AUDITING

12.1 System Monitoring. The Firm reserves the right to monitor all use of Firm computing resources, including email, internet access, file transfers, and system access logs. Personnel have no expectation of privacy when using Firm systems.

12.2 Compliance Audits. The Chief Compliance Officer shall conduct annual compliance audits of: (a) document retention practices; (b) access control effectiveness; (c) employee training completion; (d) third-party vendor compliance; and (e) incident response readiness.

12.3 External Audits. The Firm shall engage an independent third party to conduct a comprehensive information security assessment at least every two (2) years.

12.4 Audit Reports. Audit findings shall be reported to the Managing Partners Committee within thirty (30) days of completion, with remediation plans for any identified deficiencies.

Section 13. DISCIPLINARY ACTIONS

13.1 Violations. Violations of this Policy may result in disciplinary action, up to and including: (a) verbal warning; (b) written warning; (c) suspension of system access; (d) suspension of employment; (e) termination of employment; and/or (f) referral for criminal prosecution.

13.2 Severity Assessment. The severity of the disciplinary action shall be determined based on: (a) the nature and extent of the violation; (b) whether the violation was intentional or negligent; (c) the impact on clients, the Firm, or third parties; (d) prior violations; and (e) the individual's cooperation with the investigation.

13.3 Reporting Violations. Personnel who become aware of policy violations must report them to the Chief Compliance Officer or through the Firm's anonymous ethics hotline. Retaliation against good-faith reporters is strictly prohibited.

Section 14. POLICY REVIEW, UPDATES, AND TERMINATION CONDITIONS

14.1 Annual Review. This Policy shall be reviewed at least annually by the Chief Compliance Officer and

the Managing Partners Committee to ensure continued relevance and effectiveness.

14.2 Updates. Updates to this Policy shall be communicated to all personnel via email and posted on the Firm's intranet. Material changes require approval by the Managing Partners Committee.

14.3 Policy Termination. This Policy may be terminated or replaced only by a written resolution of the Managing Partners Committee. Upon termination of this Policy, all records subject to the retention schedule must continue to be retained until the applicable retention periods have expired.

14.4 Questions. Questions regarding this Policy should be directed to:

Katherine M. Hargrove
Chief Compliance Officer
Hargrove & Associates LLP
khargrove@hargrovelaw.com
Direct: (202) 555-0571

Section 15. GOVERNING LAW AND JURISDICTION

15.1 Governing Law. This Policy and any disputes arising hereunder shall be governed by the laws of the District of Columbia.

15.2 Jurisdiction. Any legal action related to this Policy shall be brought in the federal or state courts located in the District of Columbia.

15.3 Indemnification. The Firm shall indemnify any partner, employee, or agent who, in good faith, takes action in furtherance of this Policy, including reporting suspected violations, issuing Legal Holds, or authorizing document destruction in accordance with the retention schedule, from and against any claims, damages, losses, and reasonable attorneys' fees arising from such actions.

APPROVED AND ADOPTED:

By: _____
Name: Katherine M. Hargrove
Title: Chief Compliance Officer
Date: January 1, 2026

By: _____
Name: Thomas E. Hargrove III
Title: Managing Partner
Date: January 1, 2026