Deihm Professional Services, LLC

Precision. Compliance. Confidence

Deihm Professional Services, LLC

Data Security and Record Retention Policy

Effective Date: August 1, 2026

Last Update: July 28, 2026

Document Control

Document Information	Details
Document Title	Data Security & Record Retention Policy
Document Owner	Deihm Professional Services, LLC
Responsible Party	Principal & Chief Consultant
Document Number	DPS-PRI-002
Effective Date	August 1, 2026
Current Version	Version 1.0
Review Frequency	Annual or as Required
Next Review Date	June 1, 2027
Classification	Internal & Client-Facing
Approved By	Principal & Chief Consultant
Supersedes	N/A (Initial Release)

Revision History

Version	Date	Description of Changes	Author/Approver
1.0	July 2026	Initial release of comprehensive Data Security & Record Retention Policy covering notary, RON, loan signing, process serving, legal support, consulting, and compliance services.	Tara Deihm
1.1	_____	_____	_____
1.2	_____	_____	_____
1.3	_____	_____	_____

Document Control Statement

Controlled Document

This document is a controlled document of Deihm Professional Services, LLC.

Printed copies, downloaded copies, emailed copies, and shared electronic copies are considered uncontrolled unless verified against the current approved version maintained by Deihm Professional Services, LLC.

This policy establishes the Company's standards for the collection, storage, protection, retention, disclosure, and disposal of business, client, notarial, loan signing, process serving, Remote Online Notarization (RON), consulting, compliance, and administrative records.

The Company reserves the right to modify, update, replace, or retire this document at any time to reflect operational changes, legal requirements, regulatory developments, technology changes, or business needs.

Users are responsible for ensuring they are referencing the most current approved version.

Contents

Policy Summary

This expanded policy describes how Deihm Professional Services, LLC ("Service Provider," "DPS," "we," "our," or "us") protects, uses, stores, retains, and disposes of client information and service records across all active service lines. It expands the prior Remote Online Notarization ("RON") exhibit into a broader data security and retention framework for in-person/mobile notary services, loan signing services, RON, process serving and legal support, and consulting/compliance services.

- Protect confidential client, signer, borrower, legal, and business information using appropriate administrative, technical, and physical safeguards.
- Retain records only for the period required by law, regulation, contract, platform requirements, client instructions, or legitimate business need.
- Limit collection and access to what is necessary to deliver the service, document the transaction, support billing, respond to disputes, and satisfy compliance obligations.
- Use secure third-party systems and service providers only where their role is necessary to support scheduling, communication, document execution, storage, or service delivery.
- Maintain clear procedures for record handling, secure disposal, incident response, and periodic review.

1. Purpose

The purpose of this policy is to establish a consistent data security and record retention framework for all services offered by DPS. The policy supports confidentiality, documentation integrity, client trust, responsible use of technology, and audit-ready operational practices.

This policy is designed to work together with DPS service agreements, privacy notices, terms and conditions, client instructions, vendor/platform terms, and any service-specific exhibits or statements of work.

2. Scope of Covered Services

This policy applies to information collected, created, received, transmitted, processed, stored, or disposed of in connection with the following service areas:

- In-person and mobile notary services, including acknowledgments, jurats, oaths/affirmations, and other notarial acts authorized under applicable law.
- Loan signing services, including document handling, signing appointments, lender/title communications, appointment confirmations, shipping records, and related administrative records.
- Remote Online Notarization services, including platform-based identity verification, audio-visual session records, electronic journal entries, digital signatures, electronic seals, and audit trails.

- Process serving and legal support services, including service requests, case instructions, due diligence notes, service attempts, proof/affidavit preparation, client communications, and related evidence of service.
- Consulting and compliance services, including policy development, operational documentation, master data management support, impact data services, NMTC project compliance support, reporting materials, workpapers, and client deliverables.
- Client portal, scheduling, email, storage, and communication tools used to support the above services.

3. Guiding Principles

- Minimum necessary collection: DPS collects and retains only the information reasonably needed to perform the requested service, comply with recordkeeping duties, confirm identity, process payment, support client communications, or defend the integrity of a completed transaction.
- Confidentiality by default: Client, signer, borrower, case, and business information is treated as confidential unless the client has authorized disclosure, disclosure is necessary for service delivery, or disclosure is required by law, subpoena, court order, agency request, or other legal obligation.
- Need-to-know access: Access to information is restricted to the owner, authorized personnel, approved vendors, applicable platforms, and client-authorized parties who need access to complete the engagement.
- Security proportionality: Safeguards are selected based on the sensitivity of the information, the service context, the systems used, and the potential risk of unauthorized access, alteration, disclosure, or loss.
- Retention discipline: Records are retained for the required or approved period and securely disposed of when no longer needed, unless a litigation hold, regulatory inquiry, client instruction, or contractual requirement requires continued retention.
- Document integrity: DPS protects records against unauthorized alteration and maintains audit trails, logs, signed certificates, affidavits, receipts, or other evidence where appropriate.

4. Information Categories

Depending on the service, DPS may handle the following categories of information:

Information Category	Examples	Primary Service Context
Personal/contact information	Name, address, phone, email, appointment details, authorized representative details	All services
Identity verification information	Government ID review details, credential analysis result, KBA result, credible witness details, journal identification method	Notary, RON, loan signing
Transaction and document information	Document description, transaction type, notarial act type, title/escrow instructions, executed documents, receipts, shipping/tracking records	Notary, loan signing, RON
Audio-visual and electronic records	RON session recording, electronic journal entry, platform audit trail, electronic signature/seal evidence	RON
Case/legal support information	Service instructions, addresses to attempt, attempt notes, photos where permitted, affidavits/proofs of service, court/client references	Process serving and legal support
Business and compliance information	Policies, procedures, reports, data files, compliance workpapers, project records, client deliverables	Consulting and compliance
Billing and administrative records	Invoices, receipts, payment status, service agreement, engagement notes, client communications	All services

5. Administrative Safeguards

- Maintain written policies, procedures, service terms, agreements, and client-facing statements that describe how information is handled.
- Review service workflows before launch or material change to identify where sensitive information is collected, stored, transmitted, or shared.

- Use standardized intake, appointment, signing, case, and delivery procedures to reduce unnecessary copying, inconsistent labeling, or uncontrolled storage.
- Separate client records by matter, engagement, transaction, or service type where practical.
- Maintain version control for operational policies and client-facing documents that govern data security, retention, privacy, or service delivery.
- Require vendors, platforms, and technology providers to support secure access, retention, recovery, and export practices appropriate to the service.

6. Technical Safeguards

- Use secure accounts, password protection, multi-factor authentication where available, and role-appropriate access controls for business systems.
- Use business email, client portal, approved signing platforms, or secure file-sharing methods for sensitive documents rather than personal or unmanaged channels.
- Protect devices used for business purposes with endpoint security, operating system updates, security patches, device lock settings, and other commercially reasonable controls.
- Use encryption in transit for cloud-based platforms and secure websites where supported by the provider.
- Maintain backup, recovery, or platform export options for critical business records where supported by the selected system or vendor.
- Avoid storing complete government identification numbers, Social Security numbers, account numbers, or other sensitive identifiers unless retention is legally required, platform-controlled, or specifically necessary for the service.

7. Physical Safeguards

- Secure paper documents, notary journals, stamps/seals, shipping materials, and service records when not actively in use.
- Limit visibility of client documents during mobile appointments, public meetings, shared workspaces, or field activities.
- Transport client records in a controlled manner and avoid leaving confidential documents unattended in vehicles or public areas.
- Use secure disposal methods such as shredding for paper records and secure deletion for electronic files when records reach the end of their retention period.
- Immediately document and escalate suspected loss, theft, misdelivery, unauthorized access, or unauthorized disclosure.

8. Service-Specific Controls

8.1 In-Person and Mobile Notary Services

- DPS records notarial acts in the notary journal in chronological order and makes journal entries contemporaneously with performance of the notarial act.
- Journal entries include the required service details, such as date/time, document description and act type, signer identity information, identification method, and fee charged, as applicable.
- Client documents are handled only as needed for review, notarization, completion, return, shipping, billing, or service documentation.
- Copies of notarized documents are not retained unless required by law, necessary for business documentation, requested by the client, or required by the nature of the engagement.
- Notary seals, stamps, certificates, and journals remain under the control of the commissioned notary and are protected from unauthorized use.

8.2 Loan Signing Services

- Loan signing documents are handled according to title, lender, signing service, escrow, or client instructions.
- DPS limits document access to appointment preparation, signer presentation, completion checks, return/shipping, status reporting, invoicing, and quality control.
- Shipping receipts, appointment confirmations, completion notices, and administrative records may be retained to document service performance.
- Borrower information and transaction details are treated as confidential and are not used for unrelated marketing or unrelated business purposes without appropriate authorization.
- If a hiring party or title company requires return, deletion, or destruction of temporary copies, DPS follows the documented instruction unless retention is required for legal, regulatory, or dispute-related reasons.

8.3 Remote Online Notarization

RON services use an approved third-party electronic notarization platform or equivalent system designed to support secure digital transactions, identity verification, audio-visual recording, electronic signatures, electronic seals, and audit trails.

- RON sessions are conducted through communication technology that allows real-time audio-visual interaction and supports identity verification by personal knowledge, credible witness, or approved identity-proofing methods.
- Where required, identity verification may include credential analysis, knowledge-based authentication, biometric tools, or other platform-supported identity-proofing services.
- The platform creates or maintains an audio-visual recording of the notarization session and associated transaction records.
- RON certificates should reflect that the notarial act involved the use of communication technology where required by applicable law or platform workflow.

- DPS relies on the RON platform provider for platform infrastructure, recording storage, audit trail generation, transaction security, export tools, data center controls, and applicable security certifications.

8.4 Process Serving and Legal Support

- Case information is collected and used only for service, attempted service, proof preparation, client communication, billing, and related legal support tasks.
- Service notes, attempt history, addresses, photographs, affidavits, proofs, timestamps, and delivery confirmations are handled as case records and protected from unnecessary disclosure.
- DPS does not disclose service strategy, case details, or recipient information to unauthorized parties.
- If court rules, client instructions, agency requirements, or matter-specific legal obligations require retention, filing, transmission, or destruction practices that differ from this policy, the stricter or engagement-specific requirement controls.
- Process serving records may be retained to support proof of service, client questions, dispute response, billing review, and service history.

8.5 Consulting and Compliance Services

- Consulting files may include client business records, operational documents, data files, policies, reports, compliance workpapers, project deliverables, meeting notes, and related communications.
- DPS limits access to consulting records to the engagement team, client-authorized stakeholders, and vendors or platforms necessary to complete the work.
- Drafts, reports, analyses, templates, and client-specific materials are treated as confidential client work product unless designated otherwise in the engagement agreement.
- Retention of client deliverables and workpapers may be adjusted by statement of work, service agreement, grant/reporting requirements, client instruction, or applicable legal/regulatory obligation.
- Where DPS receives sensitive data sets, DPS seeks to minimize data fields, avoid unnecessary direct identifiers, and document any client-requested data handling instructions.

9. Third-Party Platforms and Vendors

DPS may use third-party providers to support service delivery, including RON platforms, Microsoft 365/SharePoint/Teams/Outlook/Bookings, secure storage, signing platforms, payment processors, shipment providers, endpoint security, VPN, IT support, and similar business systems.

Third-party platforms are responsible for their own infrastructure, certifications, data center controls, retention tools, access controls, and service availability. DPS selects business-appropriate providers, but does not control every aspect of provider infrastructure or vendor operations.

- Vendor access should be limited to the purpose for which the vendor is used.
- Vendor records should be reviewed or exported as needed to support DPS retention duties.
- Client-facing agreements should disclose where a third-party platform materially affects record storage, identity verification, audio-visual recording, scheduling, communication, payment, or document execution.
- When changing vendors, DPS should evaluate export, migration, deletion, and retention continuity before discontinuing the platform.

10. Record Retention Schedule

The following schedule establishes baseline retention expectations. A longer period applies if required by law, regulation, court order, subpoena, litigation hold, agency request, contract, client instruction, insurance need, audit requirement, or documented business necessity. A shorter period may apply only when legally permitted and documented.

Record Type	Examples	Baseline Retention	Notes / Trigger
Notary journal records	Journal entries for all notarial acts	Maintain according to Pennsylvania notary law; deliver to the required county office upon commission termination events, when applicable.	Do not destroy while retention or delivery duty applies.
RON audio-visual recordings	Recorded RON session, platform recording metadata	Minimum 10 years, unless a longer period is required.	Confirm export/access procedures with platform provider.
RON electronic transaction records	Electronic journal, audit trail, signed/notarized electronic file, platform transaction evidence	At least as long as required by applicable RON law, platform requirements, service agreement, or associated recording retention.	Maintain linkage to transaction, signer, and notarial act.
In-person/mobile notary admin file	Appointment confirmation, receipt, communication, service notes	3 years after service completion, unless needed longer.	Do not retain unnecessary copies of full client documents.
Loan signing service file	Order confirmation, scanback/shipping proof, completion notice, invoice, communication	7 years after service completion, unless hiring party	Loan package copies should be returned/deleted/destroyed per hiring party instructions

		requires different handling.	unless retention is required.
Process serving case file	Service request, attempt notes, photos where permitted, affidavit/proof, communication, invoice	7 years after matter closure or final invoice, unless client/court rules require a different period.	Retain enough to support proof of service and dispute response.
Consulting/compliance engagement file	SOW, reports, workpapers, client data extracts, deliverables, communications	7 years after engagement close, unless contract or regulatory need requires different handling.	Sensitive data exports may be deleted sooner when no longer needed.
Client portal/resource access records	Portal activity, permissions, library content, client-uploaded files	Retain while account, matter, service, or resource need remains active; review periodically.	Remove inactive or unnecessary access.
Billing/accounting records	Invoices, receipts, payment confirmations, expense support	7 years after fiscal year close or as required by tax/accounting rules.	Coordinate with accounting/tax retention requirements.
Marketing inquiries / non-client leads	Website or inquiry form, general email inquiry, declined service request	2 years from last interaction unless converted to client record or opt-out/deletion request applies.	Do not retain sensitive documents from prospects unless necessary.
Incident/security records	Loss/theft reports, access issues, breach review notes, corrective actions	7 years after closure or longer if related to legal matter.	Document facts, response, notifications, and remediation.
Superseded policies and templates	Prior versions of policies, pricing guides, terms, service exhibits	7 years after superseded, or longer if tied to active contracts.	Retain version history to support auditability.

Retention control rule

If two requirements apply to the same record, DPS follows the longer retention period unless counsel, client instruction, or controlling law requires a different action. Records subject to a hold are not destroyed until the hold is released.

11. Secure Disposal

Records that have reached the end of their retention period and are not subject to a hold should be securely destroyed or deleted using a method appropriate for the record type and sensitivity.

- Paper records containing confidential or personal information should be shredded or otherwise securely destroyed.
- Electronic records should be deleted from active systems and, where practical, removed from shared folders, local devices, temporary folders, and synced storage.
- Platform-based records should be deleted, archived, exported, or retained according to platform capability, legal requirements, and documented service needs.
- Destruction of significant business records should be documented where appropriate, including date, record category, method, and person responsible.

12. Litigation Holds, Client Holds, and Regulatory Requests

DPS suspends ordinary destruction when it becomes aware of a dispute, threatened claim, subpoena, court order, agency request, audit, investigation, client hold notice, insurance matter, or other reason to preserve records.

- Holds apply to paper records, electronic records, emails, messages, platform records, recordings, signed documents, workpapers, and metadata where relevant.
- Records subject to a hold may not be destroyed, altered, overwritten, or deleted until the hold is released.
- DPS documents the hold reason, affected record categories, hold start date, responsible party, and hold release date.

13. Incident Response and Reporting

DPS treats suspected loss, theft, unauthorized disclosure, unauthorized access, altered records, misdirected communication, compromised credentials, device loss, or vendor security event as a security incident requiring review.

- Identify the affected record, system, service, client, matter, and data category.
- Contain the issue by revoking access, changing passwords, disabling links, contacting the vendor, retrieving documents, or securing devices as appropriate.

- Preserve relevant evidence, including logs, messages, platform notices, screenshots, mail headers, shipment records, or access records.
- Assess whether client notice, vendor escalation, legal review, insurance notice, regulatory reporting, or journal loss/theft reporting is required.
- Document corrective action and update procedures when the incident reveals a control gap.

14. Client Access, Return, and Deletion Requests

Clients may request access to their deliverables, administrative records, or engagement files where appropriate and legally permissible. DPS may authenticate the request, confirm authority, review confidentiality limits, and determine whether the record can be produced, returned, deleted, or retained.

DPS may decline deletion or return requests when records must be retained for legal, notarial, contractual, accounting, insurance, dispute, platform, or audit purposes.

15. Confidentiality and Permitted Use

- DPS uses client and service records only to deliver services, maintain business operations, document compliance, communicate with authorized parties, process payment, improve procedures, respond to inquiries, and satisfy legal or contractual obligations.
- DPS does not sell client documents, signer information, borrower information, case information, or consulting data.
- DPS does not disclose confidential information to unauthorized persons except as required for service delivery, client authorization, vendor support, legal compliance, regulatory request, collection, dispute response, or safety/security need.
- If a client requests use of a particular communication channel that is less secure than DPS-preferred methods, DPS may document the client instruction and limit sensitive information where practical.

16. Policy Review and Version Control

This policy should be reviewed when DPS adds a service line, changes a material platform, updates its client portal or document storage structure, changes vendor relationships, receives a security incident, modifies service agreements, or identifies a new legal/regulatory requirement.

Version	Date	Reviewed By	Summary of Changes
1.0 Draft	[Insert date]	Principal & Chief Consultant	Expanded RON data security and retention policy to all services.

17. Regulatory and Source Alignment

This policy is aligned with the operational requirements identified in the predecessor RON policy and with Pennsylvania notary recordkeeping and remote notarization requirements. Specific requirements should be verified against current law, Department of State guidance, selected platform terms, and counsel review before final adoption.

- Pennsylvania notary journal requirements: 57 Pa.C.S. § 319.
- Pennsylvania remote notarization guidance: Pennsylvania Department of State Remote Notarization General Information and Requirements.
- Predecessor source document: “Data Security and Record Retention – Remote Online Notarization Platform.”

18. Acknowledgment / Agreement Exhibit Option

If used as an attachment to a service agreement, the following acknowledgment may be retained or adapted:

Deihm Professional Services, LLC	Client / Business Client
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix A: Client-Facing Short Form Statement

DPS protects client, signer, borrower, case, and business information using reasonable administrative, technical, and physical safeguards. Records are collected and retained only as needed to deliver services, comply with notarial and legal requirements, document service performance, support billing, respond to disputes, or satisfy contractual obligations. Remote Online Notarization records, including audio-visual recordings, are retained in accordance with applicable Pennsylvania requirements and platform capabilities. DPS does not sell client documents or confidential information and uses third-party platforms only where needed for scheduling, communication, security, payment, document execution, storage, or service delivery.