



NEIHOFF LEGAL SERVICES LLC

DIGITAL FILE MANAGEMENT & SECURITY POLICY

Purpose: This policy describes the technical, administrative, and physical safeguards Neihoff Legal Services, LLC uses to protect sensitive client data and ensure compliance with Rule 1.6, Confidentiality of Information, and Rule 5.3, Responsibilities Regarding Nonlawyer Assistants, of the Illinois Rules of Professional Conduct.

1. DATA ENCRYPTION & STORAGE INFRASTRUCTURE

Zero-Knowledge Cloud Infrastructure: All active digital case files are stored on enterprise-grade, secure cloud storage platforms (e.g., OneDrive for Business or SharePoint). Accessing files via unencrypted, consumer-grade cloud solutions is strictly prohibited.

Encryption Standards: Substantive data, including legal attachments, pleadings, and personal identifiers, is protected using AES 256-bit encryption at rest and SSL/TLS protocols during transit.

Workstation Protections: Local hard drives on company computers utilize hardware-based full-disk encryption (e.g., BitLocker for Windows 11). If physical hardware is lost or compromised, all locally cached data remains completely inaccessible.

2. ACCESS CONTROL & AUTHENTICATION

Mandatory Multi-Factor Authentication (MFA): Every portal entry, personal email forwarder, password manager, and cloud repository holding firm documentation requires time-based authentication codes or biometric verification to gain access.

Workstation Environment: All contract services are performed out of a secure, dedicated home office environment. Workstations are locked automatically when unattended to prevent unauthorized local visibility.

Siloed Firm Storage: Case materials are organized by unique law firm directories. Files from different hiring attorneys are kept completely segregated to guarantee zero cross-exposure of client data.

Strong Password Protocols: Workstation and cloud passwords must meet strict complexity requirements and are rotated quarterly via a secure password manager.

3. FILE TRANSFER & COMMUNICATION PROTOCOLS

Secure Document Execution: Document signings, certifications, and onboarding agreements are handled using industry-standard e-signature platforms (e.g., Adobe Acrobat Sign) to preserve tamper-evident audit trails.

No Unencrypted Email Delivery: Highly sensitive data, such as Social Security Administration records, corporate financials, or medical histories, will not be sent via unencrypted standard email channels.

Portal-First Transfer: Files are updated and exchanged directly through the hiring firm's preferred legal practice management system (e.g., Clio or MyCase) or via password-protected, time-expiring encrypted sync links.

Network Security Restrictions: All Business operations are conducted on private networks. Using public or unencrypted Wi-Fi networks (e.g., public spaces, hotels) is strictly forbidden unless routed through a commercial Virtual Private Network (VPN).

4. RETENTION, ARCHIVING, & SECURE DESTRUCTION

Strict Preservation Window: In accordance with Section 5 of the Master Agreement, active case files are preserved for a designated period following final invoicing to allow for verification of delivery. Unless otherwise agreed in writing via a Scope of Work (SOW), active client documents are retained for exactly 90 days following the final invoice of a completed project.

Prompt Return of Records: Upon completion of services, all final drafts and case assets uploaded are fully synced to the hiring firm's primary repository.

Digital Data Erasure/Shredding: Once a file is closed and fully synced to the hiring attorney's systems, all temporary local downloads, cached project folders, and local data copies are permanently destroyed. This ensures data cannot be recovered or extracted.

Physical Document Disposal: Any physical documents in our possession are cross shredded on-site.

5. INCIDENT RESPONSE & BUSINESS CONTINUITY

Regular Backup Routines: Automated, incremental backups are executed daily to an isolated, encrypted off-site server to prevent data loss from system failures.

Breach Notification Guarantee: In the highly unlikely event of a suspected or confirmed security anomaly, Neihoff Legal Services, LLC will notify the affected supervising attorney in writing within 24 hours of discovery to ensure immediate mitigation and compliance with Illinois data breach notification laws.

Neihoff Legal Services LLC
Shawna Neihoff
P.O. Box 195, St. David, IL 61563
(217) 816-0801 Call or Text
shawna@neihofflegalservices.com
www.neihofflegalservices.com