BROTHERLY
TECHNOLOGY

LEGAL IT CHECKLIST

# The Law Firm Data Security Checklist

Confidentiality obligations translated into the specific technical controls your firm needs in place.

| | |
|---|---|
| 01 | **Encryption and access rules for privileged material** |
| 02 | **Retention policies that survive e-discovery** |
| 03 | **Secure client file sharing that staff will actually use** |

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

**Prepared by Brotherly Technology**
Owner-led IT, security, and compliance support.

**15-MINUTE ASSESSMENT**

# Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

| | |
|---|---|
| [ ] Matters and clients are classified for confidentiality, conflict, contractual, and regulatory needs. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Access follows matter teams and need-to-know restrictions with documented exceptions. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] MFA covers email, document systems, remote access, cloud apps, and privileged accounts. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Endpoints, portable devices, backups, and supported storage use managed encryption. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Sensitive transmission uses approved portals, secure links, or encrypted methods. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] External sharing expires, is attributable, and can be revoked. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Departures and matter changes remove access, sessions, forwarding, shared links, and devices. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Audit logs and alerts cover high-risk access, sharing, deletion, and administrator events. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Retention schedules align with legal holds, client terms, ethics, and applicable law. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Legal holds suspend ordinary disposal across relevant systems and custodians. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Backups are isolated and tested for matter-level and system-level recovery. | [ ] Yes<br>[ ] Partial<br>[ ] No |
| [ ] Incident response includes privilege, client notification, insurer, evidence, and alternate communications. | [ ] Yes<br>[ ] Partial<br>[ ] No |

**Quick score:** Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

CONFIDENTIALITY CONTROLS

# Protect privileged material without blocking the work

Make the secure method the easiest approved method. Pair role-based matter access with encryption, controlled sharing, and visible ownership.

| Area | Rule | Evidence |
|---|---|---|
| **Matter access** | Access by approved team and need-to-know role | Matter roster, approval, review |
| **Privileged admin** | Separate admin identities and limited elevation | Admin report, logs, review |
| **At-rest encryption** | Managed encryption for endpoints, storage, backups, portable media | Coverage and recovery-key evidence |
| **Transmission** | Approved portal/link or encrypted channel for sensitive material | Settings, sharing report, training |
| **External sharing** | Named recipient, least access, expiry, revoke, audit | Link report and periodic review |
| **Remote work** | Managed device, secure access, privacy and local-storage rules | Device and conditional-access reports |

Avoid broad 'all attorneys' or 'all staff' access when ethical walls, sensitive matters, or client terms require narrower control.

RETENTION AND SHARING

# Make disposal defensible and legal holds reliable

Retention must operate across document management, email, chat, file shares, cloud apps, exports, archives, mobile devices, and backups.

| | |
|---|---|
| 1 | Create a schedule by record category, matter status, client term, jurisdiction, and business need; assign an approver. |
| 2 | Map each category to systems, custodians, archives, exports, backups, and disposal method. |
| 3 | Define legal-hold intake, custodian acknowledgement, preservation, monitoring, release, and evidence. |
| 4 | Configure secure sharing around real client workflows with templates, expiry defaults, and easy mobile access. |
| 5 | Test one hold and one matter close; verify search, preservation, access removal, export, and eventual disposal. |

## What to watch for

**WATCH:** A policy lists years but is not configured in the systems holding the records.

**WATCH:** Legal holds depend on each employee remembering not to delete.

**WATCH:** Client files are emailed because the portal is difficult to use.

**WATCH:** Public links do not expire or identify the recipient.

**WATCH:** Backups are treated as the retention archive without a recovery or disposal plan.

MAKE IT ACTIONABLE

# Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

| | | |
|---|---|---|
| **NOW** | Name the owner and confirm the current state. | ________________________ |
| **NEXT 7 DAYS** | Fix the highest-risk gap or gather the missing evidence. | ________________________ |
| **NEXT 30 DAYS** | Complete the remaining quick wins and set review dates. | ________________________ |
| **NEXT QUARTER** | Test the process, document results, and assign improvements. | ________________________ |

**Notes / decisions / questions for your provider**

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

**Want a second set of eyes? Book a free consultation at [brotherlytechnology.com/contact/](brotherlytechnology.com/contact/) or call 404-907-1005.**

**Reference points:** ABA Formal Opinion 477R: americanbar.org | NIST Cybersecurity Framework 2.0: nist.gov/cyberframework

This checklist is educational and is not legal, ethics, e-discovery, or compliance advice. Requirements vary by jurisdiction, client, matter, contract, and law. Confirm obligations with qualified counsel and the firm's responsible professionals.