

A PRACTICAL SECURITY GUIDE FOR IT ADMINISTRATORS

Securing the Small Law Firm

The five control domains, the technical assessment that proves them, and a 90-day plan to close the gaps, for firms running PCLaw and Time Matters on-premises.

For firms of 1–20 attorneys running PCLaw and Time Matters

<div>EDITION</div> <div>United States & Canada · 2026</div>	<div>PREPARED FOR</div> <div>IT Administrators & Managing Partners</div>
<div>WHAT IS INSIDE</div> <div>5 Domains · 25-Point Checklist · 90-Day Roadmap</div>	<div>STANDARDS</div> <div>NIST CSF 2.0 · CIS v8.1 · ABA 512 · PIPEDA</div>

Where small firms are exposed, and how to close the gap

Small law firms are not small targets. They hold privileged communications, trust account funds, and personal client information, yet most firms of 1 to 20 attorneys operate without a dedicated security team, so the controls protecting this data are often misconfigured, outdated, or simply absent.

This guide is built for the IT administrator at a small firm running PCLaw or Time Matters on-premises, and it translates complex regulatory and technical obligations into controls you can verify and evidence. On-premises software gives a firm direct control over its data, but that advantage is only realized when the on-premises environment itself is properly secured.

01 The Five Control Domains

Identity, network and endpoint, data and backup, AI and SaaS, incident response

02 Technical Control Checklist

25 controls with what to verify and how to evidence each one

03 90-Day Remediation Roadmap

Three phases sequenced by risk priority, at a comfortable pace

HOW TO USE THIS GUIDE

The 90 days in the roadmap are a comfortable framework, not a deadline. Firms that can move faster should, and firms with competing demands can extend the timeline. What matters most is sequence: address the HIGH RISK findings first, because those controls are most directly tied to breach containment and to demonstrating compliance with bar and regulatory obligations.

01 PART ONE The Five Control Domains

These five domains are the core security architecture for a small firm running on-premises legal software. Each is grounded in NIST CSF 2.0 control families and CIS Controls v8.1 safeguards.

1

DOMAIN ONE

Identity & Access Management

Compromised credentials are the entry point for the majority of law firm breaches. The Verizon 2025 DBIR reports that 88% of web application attacks involve stolen credentials, so identity controls are the highest-leverage investment available to a small firm IT administrator.

Individual Accounts — No Shared Logins

Every person must have a uniquely assigned login for every system: PCLaw or Time Matters, Windows Active Directory, email, remote access, and any cloud tools. Shared accounts make forensic investigation impossible after a breach.

IMPLEMENTATION NOTE

In PCLaw, configure individual accounts under Administration > User Management. In Time Matters, use File > Setup > Users and Security > Users. Verify that no generic accounts ('Admin', 'Staff', 'Temp') exist with active credentials. Each account should map to a named individual and carry only the permissions required for that role.

Multi-Factor Authentication (MFA)

MFA is the single most effective control against credential theft, rendering stolen passwords useless without the second factor. Treat it as a mandatory baseline:

Microsoft 365: Enable MFA under Azure AD > Security > MFA. Enforce via Conditional Access policies.

VPN and Remote Desktop: Require MFA at the VPN gateway before any connection is permitted.

PCLaw / Time Matters: On-premises systems; MFA is enforced at the Windows login and VPN layer, not the application layer.

Offboarding — Same-Day Credential Revocation

When anyone departs, revoke credentials the same day: disable the Windows AD account, suspend email, revoke VPN certificates, and remove access to shared drives, portals, and cloud tools. Retain a signed offboarding checklist as evidence.

Privileged Access — Least Privilege

Administrative accounts for servers, firewalls, backup systems, and PCLaw/Time Matters should be separate from standard user accounts. No one should perform routine work using an admin account. Review who holds administrative access quarterly and document it.

Network & Endpoint Security

The perimeter of a small firm is typically a single firewall and a flat internal network, which is adequate only when properly hardened. The common failures are unconfigured default-deny rules, unpatched systems, and absent endpoint protection.

Firewall Configuration

Every firm with a PCLaw or Time Matters server should run a business-grade firewall with these minimums:

Default-deny inbound: Block all inbound traffic except explicitly permitted services.

Restricted egress: Limit outbound traffic to known business destinations. Unexpected outbound connections are a primary ransomware indicator.

Management plane isolation: Keep the firewall's management interface off the general user network, on a dedicated VLAN or named workstation.

Logged and reviewed: Retain firewall logs at least 90 days and review them monthly for anomalies.

Patching Cadence

Unpatched systems are the primary technical vector for ransomware. Apply critical and high-severity patches within 14 days of release and all others within 30 days, prioritizing internet-facing systems (firewalls, VPNs, email gateways).

Endpoint Protection

Automatic definition updates at least daily, with **real-time scanning** active, not just scheduled.

Centrally managed from a single console; consumer-grade antivirus with no central management is not sufficient.

Full-disk encryption (BitLocker or FileVault) on all laptops and mobile devices, with recovery keys stored off-device and remote wipe configured.

PCLAW AND TIME MATTERS – OCTOBER 2026 DEADLINE

Microsoft is retiring legacy Exchange Web Services (EWS) in October 2026. Firms on older versions that depend on EWS for calendar and task sync will lose that functionality with no automatic remediation. Verify your version against the AMP Membership supported-version matrix and contact Professional Services to confirm compatibility.

Data Protection & Backup

Data protection has two objectives: recovery from ransomware or hardware failure, and maintaining client matter records required by bar retention rules. These require different controls.

Backup Architecture – The 3-2-1 Rule

Three copies of data, on two different media types, with one copy stored offsite or offline:

Primary: Live data on the production server.

Secondary: Daily automated backup to a separate local device (NAS or external drive not permanently connected).

Offsite/Offline: A backup physically disconnected from the office network. Ransomware encrypts any destination it can reach, so an offline copy is the only reliable recovery option.

Restore Testing — Required, Not Optional

A backup that has never been tested is an assumption, not a control. Test restores at least every six months, or monthly where required by applicable law society or regulatory obligations. Document the date, system and data set restored, who performed it, recovery time, and whether the restore was complete. Retain for at least 24 months.

Data Classification

Tier 1 — Privileged / Trust Account: Client matter files, trust records, IOLTA ledgers. On-premises only or explicitly approved private storage.

Tier 2 — Confidential Firm Data: Financial records, HR files, contracts, strategy. Restricted access, encrypted at rest, access-logged.

Tier 3 — General Business Data: Public materials and general correspondence. Standard access controls.

Retention and Deletion

Backup retention covers the full bar-required period (typically five to seven years after matter close) for Tier 1 and Tier 2 data. Deletion is documented with a destruction certificate at end of retention.

4

DOMAIN FOUR

AI & SaaS Risk

AI tools and cloud SaaS platforms are rapidly expanding the number of places where law firm data can be exposed. Many of these risks are self-inflicted: a lawyer pastes a privileged memo into a public AI tool, or a platform stores client data in a foreign jurisdiction without the firm realizing it.

Approved Tool Register

Maintain a written register of approved tools (AI assistants, cloud storage, add-ons, communication platforms). Any tool not on the register must not be used for client work. Capture tool name, vendor, data processing location, security terms, and the date and reviewer of the last review. This supports compliance with SOC 2, GDPR, and CCPA where they apply.

AI-Specific Controls

No privileged data in public AI: No client-identifying information, matter facts, unpublished documents, or trust details in public tools (ChatGPT, Gemini, Perplexity, or similar).

Human review mandatory: A licensed attorney reviews all AI-generated content before use.

Named accounts only: Individually assigned accounts, not shared or anonymous sessions.

Logging where available: Enable compliance logs of prompts and sessions on enterprise plans.

TURN OFF AI TRAINING AND CONFIRM DATABASE ACCESS

Before any AI tool is used with firm information, confirm that any 'training', 'model improvement', or data-retention setting is turned off; many tools enable these by default, allowing your inputs to train the vendor's models. Also confirm whether the tool reads from or writes to the PCLaw or Time Matters database. If it touches that data, verify the access is permitted under your agreement with PCLaw | Time Matters, as unauthorized interaction may breach that contract. When in doubt, contact Professional Services before connecting any AI tool.

Vendor Due Diligence — SaaS Contracts

Data residency: Where are servers located? Is data stored outside the firm's country?

Breach notification: Contractual notice within a defined window (72 hours is the standard)?

Encryption at rest and in transit, and **deletion rights** at contract termination.

Subprocessors disclosed, and **no use of customer data to train AI models** (disqualifying for Tier 1).

5

DOMAIN FIVE

Incident Response & Breach Obligations

The question is not whether a firm will face an incident, but whether it has a pressure-tested plan. Firms with documented, tested procedures contain incidents faster and are far better positioned to demonstrate compliance.

The Written Incident Response Plan

Every firm should have a written incident response (IR) plan covering at minimum:

Detection: What constitutes an incident, and what monitoring is in place to surface one?

Triage: Who performs initial assessment, and what is the first call (IT, managing partner, outside forensics)?

Containment: Isolate affected systems, revoke compromised credentials, preserve logs.

Evidence preservation: What must not be deleted or modified, and who manages chain of custody?

Notification decision: What threshold triggers client notice, who decides, and who drafts it?

Vendor escalation: Keep an accessible list of software vendor support, cyber insurer, and outside counsel.

Post-incident review: What changed, and how is remediation documented?

US and Canadian Notification Obligations

California Opinion 2020-203 requires notice when there is a 'reasonable possibility' of negative impact on the client (probability, not certainty); most US state bars have moved to a similar standard, and delay that increases harm is itself a violation. Under Canada's PIPEDA, a breach posing a 'real risk of significant harm' requires reporting to the Privacy Commissioner and notifying affected individuals as soon as feasible. All breaches, reportable or not, must be recorded in writing and retained for 24 months.

TABLETOP EXERCISES THAT PRESSURE-TEST YOUR PLAN

A plan that has never been tested is just a document. Run the plan step by step at least twice a year to keep staff aware of their roles and to update steps as tools and rules evolve. A basic scenario: 'It is Monday morning. A staff member cannot open any files on the server, and the firm suspects a ransomware incident.' Walk each step in real time to find gaps before a real incident does.

02 PART TWO Technical Control Checklist

Verify each control against the 'What to Verify' column and collect the evidence described. Any HIGH RISK finding is a priority regardless of total score.

HIGH RISK

Immediate action

MED RISK

Plan within 30 days

LOW RISK

Verify annually

Section A - Identity & Access Management

#	CONTROL	WHAT TO VERIFY	HOW TO EVIDENCE IT	RISK
1	Individual accounts	Every user has a unique login. No shared accounts in PCLaw, Time Matters, AD, or email.	Export AD user list; audit PCLaw user panel. Zero shared accounts.	HIGH
2	MFA enforcement	MFA required for email, VPN, and all cloud tools. Documented as policy.	MFA policy screenshot in M365/Google Admin. VPN config showing MFA.	HIGH
3	Same-day offboarding	Written procedure; departed users disabled same day. Evidence retained.	Last 3 offboarding records with timestamps matching departure dates.	HIGH
4	Privileged access review	Admin accounts separate from user accounts. Reviewed quarterly.	Last quarterly access review sign-off. Admin group membership list.	HIGH
5	Password policy	Min. 12 characters, complexity enforced, no reuse. Managed via GPO or IdP.	GPO export showing password policy. IdP policy screenshot.	MED

Section B - Network & Endpoint Security

#	CONTROL	WHAT TO VERIFY	HOW TO EVIDENCE IT	RISK
6	Firewall – default deny	Default-deny inbound. Rules documented and reviewed quarterly.	Firewall rule export. Change log. Last quarterly review sign-off.	HIGH
7	Patch management	Critical patches within 14 days; all patches within 30 days. Tracked.	Patch dashboard export or manual log showing last 90 days.	HIGH
8	Endpoint protection	Active, auto-updating AV/EDR on every device. Centrally managed.	Central AV console showing all devices, last update, and status.	HIGH
9	Full-disk encryption	BitLocker/FileVault on all laptops and mobile devices. Keys secured.	BitLocker status report (Get-BitLockerVolume). MDM enrollment.	HIGH
10	Network segmentation	Matter files, backups, admin interfaces on separate VLANs.	Network diagram. VLAN config. Workstation cannot reach backup share.	MED
11	Remote access VPN	VPN required for remote access. MFA at gateway. No direct RDP.	VPN config. Firewall rule blocking direct RDP from internet.	HIGH

Section C - Data Protection & Backup

#	CONTROL	WHAT TO VERIFY	HOW TO EVIDENCE IT	RISK
12	Daily backup	Automated daily backup runs and completes successfully. Logs retained.	Backup job log showing last 30 days of successful runs.	HIGH
13	Offline/offsite copy	At least one backup physically disconnected from the office network.	Description or diagram of offline destination and rotation.	HIGH
14	Restore test	Restore test within last 6 months. Result documented.	Restore record: date, system, data set, who, result, time to recover.	HIGH
15	Data classification	Tier 1/2/3 defined. Tier 1 mapped to on-premises or approved storage.	Written classification policy. Data flow diagram of Tier 1 paths.	MED
16	Retention policy	Documented retention covering bar-required windows. Legal hold exists.	Written retention policy. Legal hold workflow documentation.	MED

Section D - AI & SaaS Risk

#	CONTROL	WHAT TO VERIFY	HOW TO EVIDENCE IT	RISK
17	Approved tool register	Written list of approved tools. Staff know unapproved tools are prohibited.	Tool register document. Signed staff acknowledgment of policy.	HIGH
18	AI use policy	No privileged data in public AI, human review required, named accounts only.	Policy document. Staff training attendance. Sample review workflow.	HIGH
19	Vendor due diligence	SaaS vendors assessed for residency, encryption, breach notice, deletion.	Completed questionnaires. Contract security clauses. DPA/BUSA.	HIGH
20	Cross-border data audit	Firm knows which tools store data abroad. Clients advised where required.	Data residency documentation for each approved SaaS tool.	HIGH

Section E - Incident Response & Compliance

#	CONTROL	WHAT TO VERIFY	HOW TO EVIDENCE IT	RISK
21	Written IR plan	Covers detection, triage, containment, notification, and vendor escalation.	IR plan document. Last review/update date.	HIGH
22	Breach record log	Written log of all incidents (minor or major) for the last 24 months.	Incident log. Any reported breaches with notification evidence.	HIGH
23	Tabletop exercise	Conducted within last 12 months. Findings documented and remediated.	Tabletop notes. Action items. Follow-up evidence.	MED
24	Cyber insurance	Active coverage for breach notice, legal fees, ransomware response.	Current policy certificate. Coverage summary.	MED
25	Bar/Law Society readiness	Firm knows which rules apply, what triggers notice, and who drafts it.	Written notification decision tree or IR plan section.	HIGH

DISCLAIMER

This guide is provided for informational purposes only and does not constitute legal, regulatory, or professional security advice. Engage qualified legal counsel for jurisdiction-specific compliance guidance and a certified security professional for formal technical assessments. PCLaw | Time Matters Professional Services can provide firm-specific assessments and remediation support. Regulatory guidance may change; consult primary sources for current requirements.

PCLAW | TIME MATTERS™ PROFESSIONAL SERVICES

Ready to close the gaps in this checklist?

Our Professional Services team works directly with law firms to assess, remediate, and document the controls in this guide, and to confirm your version and AMP Membership status before the October 2026 EWS deadline.

pclawtimematters.com/professional-services • 1-800-328-2898

90-Day Remediation Roadmap

The roadmap sequences remediation by risk priority. The 90 days are a comfortable framework, not a hard deadline: move faster if you can, or extend the schedule if needed, but always work the highest-priority items first. Firms with six or more HIGH RISK findings should engage Professional Services to accelerate delivery.

PHASE 1 • DAYS 1-30

Immediate Risk Reduction

MFA	Enable MFA for Microsoft 365 or Google Workspace email and all cloud tools (2-4 hours).
Offboarding audit	Pull the AD user list. Identify and disable accounts for departed staff. Document.
Backup verification	Confirm automated daily backup runs and logs show success. If not, escalate immediately.
Version check	Confirm PCLaw/Time Matters version and AMP Membership status. Contact Professional Services if unsupported.
AI policy	Draft and distribute a one-page AI use policy. No privileged data in public AI tools.
IR plan draft	Begin a written IR plan: who to call, how to isolate systems, when to notify clients.

PHASE 2 • DAYS 31-60

Structural Hardening

Patch management	Document patch posture. Apply outstanding critical patches. Establish a 14/30-day cadence.
Firewall review	Export the rule set. Remove unused rules. Verify default-deny. Restrict management access.
Offline backup	Implement an offline/offsite rotation, physically disconnected from the network.
Endpoint audit	Verify AV/EDR on all devices. Enable full-disk encryption on all laptops. Document gaps.
Vendor due diligence	Complete questionnaires for all active SaaS tools. Flag any missing security terms.
Data classification	Draft the Tier 1/2/3 policy. Map where trust account data is stored.

PHASE 3 • DAYS 61-90

Documentation & Long-Term Governance

Restore test	Perform a documented backup restore test. Record the outcome.
Tabletop exercise	Run a ransomware scenario tabletop with the managing partner and key staff. Document findings.
Privilege review	Formal quarterly admin access review. Remove stale privileges. Document sign-off.
Retention policy	Publish a written retention schedule covering all data types. Align with bar requirements.
Professional Services	Schedule an annual security review with PCLaw Time Matters Professional Services.
Cyber insurance	Review the policy. Confirm coverage for breach notification, legal fees, and ransomware.