JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · LAW FIRMS

Law Firm IT Setup Guide: Security and Ethics in Virginia

How to set up the computers, email, network, cloud services and vendors in a small law firm so client confidences stay confidential and trust account money stays put. Each step says plainly whether a rule **requires** it or official guidance **recommends** it.

By Umair Akhtar, Founder & President, JPert INC

Published November 1, 2026
Last reviewed November 1, 2026
About a 12-minute read

JPert INC
1934 Old Gallows Road, Suite 360, Vienna, VA 22182
703-576-8200 · jpert.com
Free to share. The latest version is always at https://jpert.com/white-papers/law-firm-it-setup

Scan for the latest version

The short version

- Virginia lawyers have a duty to keep up with "the benefits and risks associated with relevant technology" (Rule 1.1, Comment [6]) and to make "reasonable efforts" to prevent unauthorized access to client information (Rule 1.6(d)). Both have applied since March 1, 2016.
- Rule 1.6's own commentary lists "the employment or engagement of persons competent with technology" as one factor in whether a firm's efforts were reasonable.
- No rule prescribes a specific technology. Reasonable efforts in 2026 look like multi-factor sign-in, encrypted devices, tested backups, careful vendor selection and a call-back rule for any wire instructions.
- Business email compromise cost U.S. victims more than $3 billion in 2025, according to the FBI. For a law firm, the fastest way to lose client money is a fake change to wire instructions.

Who this is for and how to read it

This white paper is for managing partners, firm administrators and office managers at Virginia law firms with roughly 5 to 100 people and no full-time IT department. Every recommendation is labeled:

- **REQUIRED** A rule or statute requires it today.
- **RECOMMENDED** Official guidance recommends it, or it is how firms normally show "reasonable efforts."

We cite Virginia's rule numbers, which differ from the ABA Model Rules. This is general guidance, not legal or ethics advice. For a specific question, the Virginia State Bar's ethics hotline and your own ethics counsel are the right resources.

The rules that apply today

Competence and confidentiality

REQUIRED In December 2015 the Supreme Court of Virginia added a technology comment to Rule 1.1 (Competence): "Attention should be paid to the benefits and risks associated with relevant technology." It also added Rule 1.6(d), which requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" client information. Both took effect March 1, 2016. The matching ABA Model Rules are Rule 1.1, Comment 8 and Rule 1.6(c).

Comment [19] to Virginia's Rule 1.6 lists the factors used to judge whether efforts were reasonable: how sensitive the information is, how likely disclosure is without more safeguards, the cost and difficulty of more safeguards, the effect on the lawyer's ability to represent clients, and "the employment or engagement of persons competent with technology."

Vendors, cloud storage and remote staff

Virginia's Legal Ethics Opinion 1872, "Virtual Law Office and Use of Executive Office Suites," was approved by the Supreme Court of Virginia on October 2, 2019. It says a lawyer using an outside vendor to store or handle client information must choose the vendor carefully, review its technology and terms of service, instruct it to keep information confidential, and get help from someone qualified if the lawyer cannot judge the vendor alone. It also says a lawyer "is not required, of course, to absolutely guarantee that a breach of confidentiality cannot occur." The opinion applies Rule 5.3's duty to supervise non-lawyer staff to staff who are not physically in the office.

Generative AI

The ABA's Formal Opinion 512 (July 29, 2024) applies the competence, confidentiality, communication and fee rules to generative AI tools. In practice, that means knowing where a tool sends the text you type into it before you paste in client information.

Virginia's breach law

REQUIRED Like every Virginia business, a law firm that loses unencrypted Social Security, driver's license or financial account numbers must notify affected residents and the Virginia Attorney General without unreasonable delay (Va. Code 18.2-186.6). Encrypted data is excluded unless the key was also compromised. The Attorney General can impose a civil penalty of up to $150,000 per breach.

Step 1: Accounts, passwords and multi-factor sign-in

- RECOMMENDED **Multi-factor sign-in (MFA) on email, remote access, cloud apps and every admin account.** CISA's ransomware guide asks for phishing-resistant MFA on all services, starting with email and remote access. Prefer an authenticator app, passkey or security key over text messages.
- RECOMMENDED **Long passphrases and a password manager.** Current NIST guidance (SP 800-63B, Revision 4) says passwords used alone should be at least 15 characters, should be checked against lists of leaked passwords, and should not be forced to change on a schedule unless there is a sign they were stolen.
- RECOMMENDED **One login per person and separate admin accounts.** Day-to-day work happens on standard accounts. Only a few people hold administrator rights, on separate logins.
- RECOMMENDED **Access ends on the last day.** When someone leaves, turn off email, remote access, shared passwords and building access the same day.

For a firm, the most important account is email, because it is where clients send documents and where criminals send fake wire instructions. Turn on MFA there first.

Step 2: Email and wire fraud

The FBI's 2025 Internet Crime Report recorded more than $3 billion in business email compromise losses, and Virginia ranked 10th in the country in total cybercrime losses ($476.1 million). Real estate closings, settlements and trust account disbursements are prime targets.

- RECOMMENDED **A written call-back rule.** Any new or changed wire instructions are confirmed by phone, using a number from the file or the engagement letter, never the number in the email. Tell clients in your engagement letter that you will never change wire instructions by email.
- RECOMMENDED **Email authentication.** The FTC tells businesses to publish SPF, DKIM and DMARC records so criminals cannot easily send email that looks like it came from your domain.
- RECOMMENDED **Encrypted email or a secure client portal** for sensitive documents, and external-sender tags on incoming email.
- RECOMMENDED **If money moves to a criminal, act in minutes.** Call your bank to request a recall, and report it to the FBI at ic3.gov. The FBI says its Recovery Asset Team froze about 58% of the money it tried to recover in 2025 (about $679 million).

Step 3: Computers, phones and remote work

- RECOMMENDED **Encrypt every laptop and phone** that holds work data, so a lost device is a hardware problem, not a data breach. NIST's small-business guide calls for full-disk encryption on laptops and tablets.
- RECOMMENDED **Turn on automatic updates**, and patch internet-facing systems and anything on CISA's Known Exploited Vulnerabilities list first.
- RECOMMENDED **Replace unsupported systems.** Windows 10 support ended October 14, 2025. Machines that cannot upgrade yet need Microsoft's paid Extended Security Updates, which are only available for a limited time, and should be replaced.
- RECOMMENDED **Endpoint protection that someone actually watches**, on every computer. Alerts that nobody reviews do not stop an attack.

RECOMMENDED **Remote and hybrid work.** LEO 1872 applies supervision duties to staff who work outside the office. Practical controls are firm-managed laptops (not personal home computers) for client work, MFA and a VPN or secure access service for remote connections, and a short written policy on working from home and public Wi-Fi.

Step 4: Office network and Wi-Fi

- RECOMMENDED **Separate networks** for staff computers, guest Wi-Fi, and printers, cameras and other smart devices. CISA calls for network segmentation and a current diagram of how data moves.
- RECOMMENDED **WPA3 Wi-Fi** where your equipment supports it, with a long passphrase that changes when staff leave. Guests get internet access only.
- RECOMMENDED **No remote desktop open to the internet.** CISA says remote desktop should never be exposed directly. Use a VPN or secure remote-access service with MFA.
- RECOMMENDED **A supported business firewall**, kept updated and replaced when the manufacturer stops supporting it.

Many firms share space or use executive suites. LEO 1872 discusses executive office suites directly. If you share a network with other tenants, treat it as untrusted: use your own firewall and Wi-Fi for firm devices.

Step 5: Client files, cloud services and vendors

- RECOMMENDED **Choose cloud services with care, and write down why.** Following LEO 1872, record what you reviewed for each practice management, document management, email and backup vendor: its security, its terms of service, where data is stored, and how you get your data back if you leave.
- RECOMMENDED **Limit access by matter** where your systems allow it, especially for conflicts, sealed matters and HR files.
- RECOMMENDED **Control file sharing.** Turn off "anyone with the link" sharing for client folders and review external shares regularly.
- RECOMMENDED **Vet AI tools** before anyone pastes client information into them, consistent with ABA Formal Opinion 512.

RECOMMENDED In 2022, CISA, the NSA, the FBI and allied agencies published joint guidance for organizations that use a managed service provider (MSP). It says your

contract should require MFA on every account the provider uses, least-privilege access, defined incident reporting, backup and incident-response duties, and prompt removal of the provider's access when the contract ends. Ask any IT provider, including us, to show you those terms in writing.

Step 6: Backups and staying open after an attack

- RECOMMENDED **Offline, encrypted, tested backups.** CISA's guidance is to keep offline, encrypted backups of critical data and regularly test them. Many offices follow the "3-2-1" practice (three copies, two types of storage, one off-site) to meet it.
- RECOMMENDED **Back up cloud email and files too.** Cloud services keep your data running, but they are not a full backup plan on their own. Check what is covered and for how long.
- RECOMMENDED **Test a restore** on a schedule and write down how long it took.

Court deadlines do not move because of ransomware. Decide in advance which systems must come back first, usually email, calendar and docketing, and the document management system, and how the firm will meet deadlines if they are down.

Step 7: When something goes wrong

- RECOMMENDED **Write a one-page incident plan**: who to call (your IT provider, your cyber insurer and breach counsel, your bank), how to disconnect an infected computer, and how to reach staff and courts if email is down. Keep a printed copy. NIST's incident response guidance (SP 800-61, Revision 3, April 2025) is the current federal reference.
- REQUIRED **Know your notice duties.** Virginia's breach law requires notice without unreasonable delay when covered personal information is exposed. Your duty to keep clients reasonably informed may also apply. Talk to ethics counsel about what to tell affected clients.
- RECOMMENDED **Report crimes** to the FBI at ic3.gov.

One-page setup checklist

Area	What to have in place	Status today
Ethics basis	Written note of how the firm meets Rule 1.1 Comment [6] and Rule 1.6(d)	REQUIRED
MFA	On email, remote access, cloud apps and admin accounts	RECOMMENDED
Passwords	15+ character passphrases, password manager, no forced rotation	RECOMMENDED
Wire fraud	Written call-back rule; clients told you never change wire instructions by email	RECOMMENDED
Email	SPF, DKIM and DMARC; external tags; encrypted sending or portal	RECOMMENDED
Devices	Encrypted, auto-updated, monitored; no unsupported Windows 10	RECOMMENDED
Network	Firm firewall, separate guest Wi-Fi, no exposed remote desktop	RECOMMENDED
Vendors	Documented review of each cloud vendor (LEO 1872); MSP contract terms	RECOMMENDED
Backups	Offline or locked copy, cloud data included, restores tested	RECOMMENDED
Incidents	Printed one-page plan; breach notice process under Va. Code 18.2-186.6	REQUIRED notice, RECOMMENDED plan

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. Rule 1.6's commentary recognizes "persons competent with technology" as part of reasonable efforts; that is the role we play for law firms across Northern Virginia. Read about IT for law firms, or book a free IT assessment.

Related reading from our Chronicles: wire fraud prevention for law firms, law firm incident response plan and Microsoft 365 security for law firms.

Sources

Every recommendation above comes from these official sources, checked on November 1, 2026:

- Supreme Court of Virginia: Order amending Rules 1.1 and 1.6 (effective March 1, 2016)
- Virginia State Bar: Rule 1.6 Confidentiality of Information
- Virginia LEO 1872: Virtual Law Office and Use of Executive Office Suites
- ABA Formal Opinion 512: Generative Artificial Intelligence Tools (July 29, 2024)
- Va. Code 18.2-186.6 (breach of personal information notification)
- FBI: 2025 Internet Crime Report
- FTC: Cybersecurity for Small Business
- NIST SP 800-63B Rev. 4: Authentication and passwords
- CISA: #StopRansomware Guide
- CISA, NSA, FBI and allied agencies: Protecting against cyber threats to MSPs and their customers (AA22-131A)
- NIST SP 800-61 Rev. 3: Incident response recommendations (April 2025)
- Microsoft: Windows 10 end of support and Extended Security Updates
- Wi-Fi Alliance: Wi-Fi security and WPA3
- NIST SP 1300: Cybersecurity Framework 2.0 Small Business Quick-Start Guide

This white paper is general information about IT and security practices, not legal or ethics advice. Rules and ethics opinions change; we review this paper when they do. See our editorial policy.

FAQ

Common questions from law firms

Do Virginia ethics rules require specific cybersecurity tools?

No. Rule 1.6(d) requires reasonable efforts to prevent unauthorized access to client information, and Rule 1.1 Comment [6] requires attention to the benefits and risks of relevant technology. The rules do not name tools. Reasonableness depends on factors listed in Comment [19], including the sensitivity of the information and the cost of safeguards.

Can a Virginia law firm store client files in the cloud?

Yes, with care. Legal Ethics Opinion 1872 says lawyers must choose vendors carefully, review their technology and terms of service, instruct them to keep information confidential, and consult a qualified person if they cannot judge the vendor themselves. It does not require a guarantee that no breach can occur.

What is the single most important control for a law firm?

Multi-factor sign-in on email, paired with a written rule that any change to wire instructions is confirmed by phone using a known number. Email account takeover and fake wire instructions are among the most common ways firms and clients lose money.

Does Virginia's breach law apply to law firms?

Yes. Va. Code 18.2-186.6 applies to any business that holds covered personal information, such as Social Security or financial account numbers, and requires notice to affected residents and the Attorney General without unreasonable delay if unencrypted data is breached.

Want us to check your setup against this guide? Book a free IT assessment with our Vienna, VA team at jpert.com/contact or call 703-576-8200. We will give you a plain-English list of what to fix first.