JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · PROPERTY MANAGEMENT

Property Management IT Setup Guide: Tenant Data Security

How a small property management company should set up its office, leasing systems, payments and building technology so tenant data and rent money stay safe. Each step says plainly whether the law **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 11-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/property-management-it-setup

Scan for the latest version

The short version

- Tenant screening reports are consumer reports. The FTC Disposal Rule, which names landlords and property managers, requires disposing of them so the information cannot practicably be read or reconstructed.
- Virginia law makes tenant records confidential (Va. Code 55.1-1209), limits how leasing offices scan driver's licenses (Va. Code 59.1-443.3), and requires breach notice when personal information is exposed (Va. Code 18.2-186.6).
- Real estate fraud cost victims $275.1 million in 2025, according to the FBI. Confirm any change to an owner's, vendor's or tenant's payment details by phone.
- Cameras, door access systems and thermostats belong on their own network, with default passwords changed, away from the computers that hold tenant files.

Who this is for and how to read it

This white paper is for owners and office managers of residential and commercial property management companies with roughly 5 to 100 staff. Every recommendation is labeled:

- **REQUIRED** A law or binding rule requires it today.
- **RECOMMENDED** Official guidance from the FTC, NIST or CISA recommends it.

This is general guidance, not legal advice; ask counsel about your specific obligations.

The rules that apply today

Tenant screening reports

REQUIRED Tenant screening and credit reports are consumer reports under the Fair Credit Reporting Act. The FTC's guidance for "the landlord, or property manager or other housing provider" covers permissible purpose and adverse action notices. The FTC Disposal Rule (16 CFR Part 682) requires reasonable measures to dispose of consumer report information: shred or burn paper, and erase or destroy electronic media so the information "cannot practicably be read or reconstructed."

Virginia tenant records and ID scanning

REQUIRED Under the Virginia Residential Landlord and Tenant Act, tenant records are confidential except in listed situations (Va. Code 55.1-1209). The statute also limits a landlord's liability for a breach at a third-party records vendor unless there was gross negligence or an intentional act, which supports keeping tenant files in a reputable property management platform rather than scattered across email and shared drives. A 2026 amendment, effective July 1, 2027, adds a deadline for providing statements of charges and payments.

REQUIRED Virginia limits scanning of driver's licenses and requires scanned information to be handled and destroyed as the statute directs (Va. Code 59.1-443.3). Check your leasing office's ID scanning practice against it.

Breach notification and payments

REQUIRED Virginia's breach law (Va. Code 18.2-186.6) requires notice to affected residents and the Attorney General without unreasonable delay when unencrypted Social Security, driver's license or financial account numbers are exposed. Rental applications usually contain all three.

REQUIRED If you accept rent or fees by card, PCI DSS applies through your processor agreement. Version 4.x is in force, and its future-dated requirements became mandatory March 31, 2025.

The FTC Safeguards Rule: check whether it applies

The FTC Safeguards Rule (16 CFR Part 314) does not list landlords or property managers as covered businesses, but it does cover some real estate-related financial activities, such as settlement services. If your company lends money or performs other financial services, ask counsel whether it applies. Either way, its controls are a sensible benchmark.

Step 1: Protect rent, owner and vendor payments

- RECOMMENDED **Confirm every new or changed bank detail by phone**, using a number you already have, never one in the email. 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). The same report recorded $275.1 million in real estate fraud losses.
- RECOMMENDED **Two-person approval** for new vendors and changes to owner distribution accounts.
- RECOMMENDED **Tell tenants, owners and vendors in writing** that you will never change payment instructions by email.
- RECOMMENDED **Publish SPF, DKIM and DMARC records**, as the FTC recommends, so criminals cannot easily send rent notices that look like yours.

Step 2: 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.

Your property management platform holds tenant applications, ledgers and bank details. Turn on MFA there and in email first, and give leasing agents, maintenance staff and accounting only the access their role needs.

Step 3: Tenant files, applications and disposal

- RECOMMENDED **Keep applications and screening reports in one system**, not in email attachments, desktop folders and paper files at the same time.
- RECOMMENDED **Collect only what you need**, and set a retention schedule for applications from people who did not become tenants.
- REQUIRED **Dispose properly.** Shred paper screening reports and wipe or destroy old drives and copiers before they leave the office, as the FTC Disposal Rule requires for consumer report information.
- RECOMMENDED **Encrypt laptops and phones** used by leasing and maintenance staff, so a lost device is not a breach.

Step 4: Building systems on their own network

Cameras, door access controllers, gate systems, thermostats and smart locks are computers too. NIST's guidance for connected-device makers (NIST IR 8259, Revision 1, April 2026) notes that customers often end up administering the devices they buy.

- RECOMMENDED **Put building systems on a separate network segment** from office computers and tenant Wi-Fi. CISA calls for segmentation and for separating operational technology from IT.

- RECOMMENDED **Change every default password** and remove accounts for former staff and vendors.
- RECOMMENDED **Update firmware** and replace devices the manufacturer no longer supports.
- RECOMMENDED **Control vendor remote access** to building systems: named accounts, MFA, and access turned off when the contract ends.

Step 5: Office computers and network

- 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 **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.

Step 6: Backups and vendors

- 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.

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 7: When something goes wrong

- RECOMMENDED **Write a one-page incident plan**: who to call (your IT provider, your cyber insurer, your attorney, your bank), how to disconnect an infected computer, and how to reach staff if email is down. Keep a printed copy, and walk through it once a year. NIST's incident response guidance (SP 800-61, Revision 3, April 2025) is the current federal reference.
- REQUIRED **Know Virginia's breach law.** If unencrypted Social Security, driver's license, passport, military ID or financial account numbers of Virginia residents are exposed, Va. Code 18.2-186.6 requires notice to those residents and the Virginia Attorney General without unreasonable delay. If more than 1,000 people are notified at once, the Attorney General and the national credit bureaus must also be told. The Attorney General can impose a civil penalty of up to $150,000 per breach. Encrypted data is excluded unless the key was also compromised.

- RECOMMENDED **If money moved 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).

One-page setup checklist

Area	What to have in place	Status today
Screening reports	Permissible purpose; secure storage; proper disposal	REQUIRED (FCRA, Disposal Rule)
Tenant records	Kept confidential in one system; retention schedule	REQUIRED (Va. Code 55.1-1209)
ID scanning	Leasing office practice matches Va. Code 59.1-443.3	REQUIRED
Breach readiness	Notice process under Va. Code 18.2-186.6	REQUIRED
Card payments	Processor-hosted payments; yearly PCI self-assessment	REQUIRED (PCI DSS)
Payments	Phone call-back; two-person approval; written notice to tenants and owners	RECOMMENDED
MFA	Email, property management platform, banking, admin accounts	RECOMMENDED
Building systems	Separate network; defaults changed; vendor access controlled	RECOMMENDED
Devices	Encrypted, updated, monitored; no unsupported Windows 10	RECOMMENDED
Backups	Offline or locked copy; platform data exportable; restores tested	RECOMMENDED

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. We support property managers across Northern Virginia, from the leasing office to building networks. Read about IT for property management, or book a free IT assessment.

Related reading from our Chronicles: tenant data protection, access control system security and smart building IoT security.

Sources

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

- FTC: Using Consumer Reports, What Landlords Need to Know
- FTC Disposal Rule, 16 CFR Part 682 (eCFR)
- FTC: Disposing of Consumer Report Information? Rule Tells How
- Va. Code 55.1-1209 (confidentiality of tenant records)
- Va. Code 59.1-443.3 (scanning of driver's licenses)
- Va. Code 18.2-186.6 (breach of personal information notification)
- PCI Security Standards Council: Future-dated PCI DSS v4.x requirements
- FTC Safeguards Rule, 16 CFR Part 314 (eCFR)
- NIST IR 8259 Rev. 1: Foundational cybersecurity activities for IoT product manufacturers (April 2026)
- 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

This white paper is general information about IT and security practices, not legal advice. Rules change; we review this paper when the underlying rules or guidance change. See our editorial policy.

FAQ

Common questions from property managers

How should property managers dispose of tenant screening reports?

The FTC Disposal Rule requires reasonable measures: shred or burn paper reports, and erase or destroy electronic files and media so the information cannot practicably be read or reconstructed. The FTC's guidance names landlords and property managers specifically.

Are tenant records confidential in Virginia?

Yes. Va. Code 55.1-1209 makes tenant records confidential except in listed situations, and limits a landlord's liability for a breach at a third-party records vendor unless there was gross negligence or an intentional act.

Does the FTC Safeguards Rule apply to property management companies?

It does not list landlords or property managers as covered businesses, but it covers some real estate-related financial activities such as settlement services. If your company lends money or provides other financial services, ask counsel whether it applies.

How should building systems like cameras and door access be secured?

Put them on a separate network from office computers and tenant Wi-Fi, change every default password, keep firmware updated, replace unsupported devices, and give vendors named remote access accounts with multi-factor sign-in that end with the contract.

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.