JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · CONSTRUCTION

Construction Company IT Setup Guide: Office to Jobsite

How a small general contractor, specialty contractor or builder should set up IT across the office, the trailer and the field, so payments, project files and schedules 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/construction-it-setup

Scan for the latest version

The short version

- There is no construction-specific federal cybersecurity rule. Your requirements come from Virginia law, your contracts, your insurer and your lenders. NIST's free Cybersecurity Framework 2.0 is the best official playbook.
- Payment fraud is the biggest documented threat. Business email compromise caused more than $3 billion in reported U.S. losses in 2025; draw requests, change orders and retainage payments are natural targets.
- Jobsite phones and tablets hold drawings, photos and email. NIST's mobile device guidance (SP 800-124, Revision 2) is the official reference for managing them.
- Federal projects can change everything: drawings marked as Controlled Unclassified Information bring DoD security rules into your office.

Who this is for and how to read it

This white paper is for owners, controllers and operations managers at construction firms with roughly 5 to 100 office and field staff. Every recommendation is labeled:

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

This is general guidance, not legal advice.

The rules that apply today

- REQUIRED **Virginia's breach law** (Va. Code 18.2-186.6) applies to the personal information you hold: employee payroll and I-9 records, and subcontractor W-9 forms, which can include Social Security numbers. If unencrypted data is exposed, notify affected residents and the Attorney General without unreasonable delay.

- REQUIRED **Federal work** brings federal rules. If a contract includes FAR 52.204-21, you must meet its 15 basic safeguards. If drawings or specifications are marked as Controlled Unclassified Information on a Defense project, DFARS 252.204-7012 and NIST SP 800-171 apply. See our government contractor white paper.
- **Contracts, bonds, lenders and insurers** often add their own requirements, such as MFA, backups or wire-verification procedures. Read them; they are binding on you.

Step 1: Stop payment fraud on draws, change orders and retainage

Construction runs on large, predictable payments to and from many parties, which is exactly what email fraudsters look for. Criminals research projects, register lookalike email domains, and send convincing requests to "update" bank details.

- 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).
- RECOMMENDED **Two people approve** any new payee or changed bank details, and the person who verifies is not the person who received the request.
- RECOMMENDED **Tell owners and subcontractors in writing** that you will never change payment instructions by email.
- RECOMMENDED **Turn on MFA for email** for everyone, including field staff and project managers, since a hijacked mailbox is how most of these schemes start.
- RECOMMENDED **Publish SPF, DKIM and DMARC records**, as the FTC recommends, so criminals cannot easily send email that looks like it came from your domain.

Step 2: Accounts and passwords for office and field

- 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.

Field crews often share a tablet or a login to a project app. Give each person their own login wherever the app allows it, so you know who did what and can remove access when someone leaves the company or a subcontractor finishes.

Step 3: Jobsite phones, tablets and trailers

- RECOMMENDED **Manage company phones and tablets centrally**, following NIST SP 800-124, Revision 2: require a passcode and encryption, keep them updated, and be able to locate, lock or wipe a lost device.
- RECOMMENDED **Separate work from personal** on personal phones that get company email, so you can remove company data without touching personal photos.
- RECOMMENDED **Secure trailer and jobsite Wi-Fi** with WPA3 where supported and a strong passphrase that changes between projects. Keep subcontractor and guest devices on their own network.
- RECOMMENDED **Lock up network equipment** in trailers and change default passwords on cameras, access gates and other connected site equipment.

Step 4: 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 5: Project files, backups and cloud apps

- 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 **Know where project records live**: drawings, RFIs, submittals, photos, daily logs and estimates are often spread across email, cloud project platforms and personal phones. Pick official locations and back them up.
- RECOMMENDED **Protect bid files.** Limit access to estimates and bid documents to the people who need them.
- RECOMMENDED **Check each cloud project platform** for MFA, user roles, and how you export your data when a project closes or you change platforms.

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: 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
Payments	Phone call-back on known numbers; two-person approval; written notice to partners	RECOMMENDED
Breach readiness	Notice process under Va. Code 18.2-186.6 for payroll and W-9 data	REQUIRED
Federal work	FAR 52.204-21 safeguards; DFARS 7012 if CUI on DoD projects	REQUIRED when in contract
MFA	Email for office and field; project apps; admin accounts	RECOMMENDED
Mobile devices	Managed, encrypted, locatable and wipeable	RECOMMENDED
Jobsite Wi-Fi	WPA3, changed per project; separate subcontractor network	RECOMMENDED
Office devices	Encrypted, updated, monitored; no unsupported Windows 10	RECOMMENDED
Network	Supported firewall; no exposed remote desktop	RECOMMENDED
Project data	Official file locations; backups include cloud platforms; restores tested	RECOMMENDED

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. We support construction firms across Northern Virginia from the office to the trailer, including structured cabling and Wi-Fi. Read about IT for construction companies, or book a free IT assessment.

Related reading from our Chronicles: bid security and fraud prevention, mobile device security for construction and construction data backup.

Sources

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

- NIST Cybersecurity Framework 2.0 (CSWP 29)
- NIST SP 1300: Cybersecurity Framework 2.0 Small Business Quick-Start Guide
- NIST SP 800-124 Rev. 2: Managing the Security of Mobile Devices in the Enterprise
- FBI: 2025 Internet Crime Report
- FTC: Cybersecurity for Small Business
- Va. Code 18.2-186.6 (breach of personal information notification)
- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems
- DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting
- 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

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 construction firms

Is there a cybersecurity regulation for construction companies?

There is no construction-specific federal cybersecurity rule. Construction firms follow Virginia's breach notification law, the requirements in their contracts, insurance and loans, and, on federal projects, federal contract clauses such as FAR 52.204-21 and DFARS 252.204-7012.

How do construction companies prevent payment fraud?

Confirm every new or changed bank detail by phone using a number you already have, require two people to approve payee changes, tell partners in writing that you never change payment instructions by email, and turn on multi-factor sign-in for every mailbox.

How should jobsite phones and tablets be secured?

Manage them centrally as NIST SP 800-124 recommends: require a passcode and encryption, keep them updated, and make sure a lost device can be located, locked or wiped.

What changes when we bid on federal projects?

Federal contracts can include FAR 52.204-21's 15 basic safeguards, and Defense projects with Controlled Unclassified Information bring DFARS 252.204-7012, NIST SP 800-171 and the CMMC program into scope.

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.