# CJIS Readiness Checklist

For Pennsylvania municipalities, police departments, and the IT providers that support them. Written against FBI CJIS Security Policy v6.1.

## How to use this checklist

If your agency accesses criminal justice information (CJI) through CLEAN, NCIC, or JNET, the CJIS Security Policy applies to every system, person, and vendor that can touch that data. That includes your IT provider, a county or municipal IT department that manages the network, and contractors with unescorted access to the server room. Work through each section and check off what you can prove with documentation, not just what you believe is in place. Every unchecked box is a question to answer before your next audit.

**Dates that matter right now.** CJIS Security Policy v6.1 took effect June 25, 2026. It raised the minimum encryption key strength to 256-bit and moved vulnerability scanning to at least monthly. FIPS 140-2 cryptographic validations reached end of life on September 21, 2026, so encryption should now rely on FIPS 140-3 validated modules. Most modernized v6.x requirements move into normal audit and sanction treatment on October 1, 2027. In Pennsylvania, the Pennsylvania State Police (CLEAN Administrative Section) is the CJIS Systems Agency. Confirm with them which policy version your next audit will use.

## 1. Scope and agreements

You cannot protect CJI you have not located. Start by knowing where it lives and who can reach it.

- [ ] We have a current inventory of every system, device, application, and location where CJI is accessed, stored, processed, or transmitted, including cloud services and mobile devices.
- [ ] Every vendor with logical or unescorted physical access to CJI or CJI systems (IT provider, cloud provider, cabling or security installer) has signed the CJIS Security Addendum.
- [ ] If a non-criminal justice agency, such as county or municipal IT, manages our systems, a management control agreement is in place.
- [ ] We have a designated Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO), and both know their responsibilities.
- [ ] Our written security policies reflect the current CJIS Security Policy structure, not the older 13-area version that much online guidance still describes.

## 2. People and training

- [ ] Everyone with unescorted access to CJI or a physically secure location, including vendor staff, has completed a fingerprint-based background check.
- [ ] Security awareness training is completed before access is granted and refreshed on the required cycle, with completion records kept.
- [ ] Access is removed promptly when someone leaves or changes roles, and we can show when it happened.

## 3. Access control and identity

- [ ] Every user has a unique account. No shared or generic logins are used to reach CJI.
- [ ] Multi-factor authentication is enforced for access to CJI, including remote and vendor access.
- [ ] Access follows least privilege, and accounts and permissions are reviewed on a regular schedule.
- [ ] Sessions lock after inactivity, and repeated failed logins trigger a lockout.
- [ ] Remote access by our IT provider is logged, uses MFA, and is limited to what the work requires.

## 4. Encryption

Outside a physically secure location, CJI must be encrypted, in transit and at rest.

- [ ] CJI in transit outside a physically secure location is protected with FIPS 140-3 validated cryptography or FIPS 197 AES with at least 256-bit keys.
- [ ] CJI at rest outside a physically secure location (laptops, mobile devices, backups, cloud storage) meets the same standard.
- [ ] We have checked VPNs, firewalls, backup systems, and encrypted email tools for products that relied on FIPS 140-2 validations now past their sunset date.

## 5. Physical security

- [ ] The physically secure location boundary is defined in writing and matches how the building is used.
- [ ] Visitors and unscreened vendors are escorted, and visitor access is logged.
- [ ] Terminals and screens that display CJI are positioned so they cannot be viewed by the public.

## 6. Systems, devices, and media

- [ ] Operating systems, firmware, and applications on CJI systems are patched on a defined schedule.
- [ ] Vulnerability scans of CJI systems run at least monthly (v6.1 raised this from quarterly), and findings are tracked to remediation.
- [ ] Endpoint protection is installed, current, and monitored on every system that touches CJI.
- [ ] Laptops, tablets, and phones that access CJI are managed with mobile device management, including remote lock and wipe.
- [ ] Media containing CJI is tracked, protected in transport, and sanitized or destroyed with records kept.

## 7. Monitoring, logging, and incident response

- [ ] Security-relevant events on CJI systems are logged, reviewed, and retained as the policy requires.
- [ ] We have a written incident response plan that names who does what and when the CSA is notified.
- [ ] The plan has been tested within the last year, and lessons learned were documented.
- [ ] Backups of CJI systems are encrypted, tested by actual restore, and protected from tampering.

## 8. Microsoft 365, cloud services, and AI tools

- [ ] We know exactly which Microsoft 365 tenant type we use and whether CJI ever passes through email, Teams, SharePoint, or OneDrive.
- [ ] If CJI is in any cloud service, we have confirmed the provider's CJIS agreements and configuration cover our use in Pennsylvania.
- [ ] Cloud admin accounts are separate from daily-use accounts and protected with phishing-resistant MFA.
- [ ] CJI is never entered into AI tools (chatbots, copilots, transcription or report-writing assistants) unless the tool is inside our CJIS scope, with agreements, encryption, and logging in place.
- [ ] We have a written AI acceptable use policy that tells staff which AI tools are approved and that CJI stays out of everything else, and staff have been trained on it.
- [ ] We have confirmed that no AI vendor we use trains its models on our data.

## 9. Questions to ask your IT provider

- [ ] Have you signed the CJIS Security Addendum, and have your staff completed fingerprint-based background checks and CJIS training?
- [ ] How do your technicians access our systems, and can you show us the access logs?
- [ ] Can you produce the documentation an auditor will ask for, not just tell us it is handled?
- [ ] Do you know the difference between the v5.9.5 and v6.x control structures, and which one our next audit uses?
- [ ] How do you keep CJI out of AI tools in our environment, and what controls enforce that?

**Want a second set of eyes?** Every 3rd Element staff member is CJIS cleared, and we manage agency environments to a written standard. Schedule a free IT Environment Review at **3rdelementconsulting.com/schedule**. It takes about 30 minutes, and you get a written summary afterward.

This checklist is a readiness aid, not a compliance determination or legal advice. The FBI CJIS Security Policy and your state CJIS Systems Agency (in Pennsylvania, the Pennsylvania State Police CLEAN Administrative Section) are the authoritative sources, and state requirements may be stricter than the federal baseline. Current as of September 2026.