



COMPUTER TIES IT RESOURCE CENTER • PLANNING WORKSHEET

CJIS-Governed Environment IT Planning Worksheet

For agencies whose systems access, process, transmit, or store criminal justice information — a way to map what you have before reviewing it against current requirements.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

Requirements for these environments come from several directions at once. The FBI CJIS Security Policy, the Michigan Addendum, LEIN policy, your own agency procedures, agreements with other agencies, and whatever your vendors are contractually required to do can all apply to the same room full of equipment.

This worksheet does not tell you whether you comply with any of that. It helps you write down what you actually have, so that the review against current requirements has something to work from. In practice, most agencies find that the hardest part is not the rules. It is not having a clear picture of their own environment.

What this document is not

This is a planning aid. It is **not** a compliance assessment, a certification, an audit tool, or a substitute for your agency's required CJIS review.

The current FBI CJIS Security Policy, the Michigan Addendum, and Michigan State Police LEIN materials are the authoritative sources, and they change. All of them are linked from the Computer Ties IT Resource Center. Your agency's CJIS Systems Officer, Local Agency Security Officer, Terminal Agency Coordinator, and state contacts are the people who determine what applies to you.

How to use this document

Work through it as an inventory exercise first. Write down what exists. Do not try to judge whether each item meets a requirement while you are still finding out what you have.

Take the completed picture into your review against the current policy, and into any conversation with your state contacts or auditors.

A completed copy describes a criminal justice environment in detail. Treat it as sensitive and handle it according to your agency's own rules.

The words you will hear, and what they actually mean**CJI (criminal justice information)**

The information the policy exists to protect. Working out everywhere it actually goes is the hardest part of the job, and section 1 is about exactly that.

ORI (originating agency identifier)

The identifier assigned to your agency for access to these systems.



TAC (Terminal Agency Coordinator)

Your agency's designated point of contact for these systems and their use.

LASO (Local Agency Security Officer)

The person responsible for security matters at your agency, and the person who should be holding the completed version of this worksheet.

CSO (CJIS Systems Officer)

The state-level official responsible for administering the policy within Michigan.

Advanced authentication

The policy's own term for requiring more than a password. What the rest of the world calls multifactor authentication.

Security Addendum

The agreement that brings a private contractor under the same obligations as agency personnel. If a vendor supports your systems, ask where yours is filed.

1 Scope — Where Does It Actually Go?

Almost every difficulty in these environments traces back to scope being wider than anyone assumed. Information tends to travel: into reports, onto shared drives, through email, onto laptops, into printers, and onto phones.

- ☐ Which terminals, workstations, and mobile devices are used to access it.
- ☐ Which vehicles have equipment that touches it.
- ☐ Which software stores it, including records management, dispatch, and reporting systems.
Also anything that receives an export, a report, or an automated feed from those systems.
- ☐ Whether it ever reaches email, shared folders, or general office storage.
This is where scope quietly expands, and it is usually unintentional.
- ☐ Which printers, scanners, and copiers handle it, including anything that stores images internally.
- ☐ Whether it appears on any screen visible from a public area.
- ☐ Which staff, contractors, volunteers, and other agencies have access.
- ☐ Whether any of it leaves the building on paper, on removable media, or on a device.
- ☐ Which backups contain it, and where those backups are held.

Our agency ORI

Local Agency Security Officer

Terminal Agency Coordinator

Who else has a defined role



2 Equipment That Touches It

What it is	Where	Who uses it	Software on it	Age

3 Areas to Review Against Current Requirements

Each of these is an area where the current policy sets expectations. Use the boxes to record whether you have identified how your agency handles it, not whether you believe you comply.

Who gets in

- ☐ How people sign in, and what additional factor is required beyond a password.
- ☐ How access is granted, reviewed, and removed, including for people who change roles.
- ☐ How accounts belonging to people who leave are handled, and how quickly.
- ☐ Whether anybody shares a login anywhere in the environment.

People

- ☐ Personnel screening and fingerprint-based background checks for everyone with access.
- ☐ Security awareness training, who has to take it, and how often.
- ☐ Signed acknowledgements and any required agreements.
- ☐ Contractors, vendors, and anybody supporting the systems from outside.
There are specific expectations for private contractors supporting these environments, including a security addendum.



■ The information itself

- ☐ Encryption of information as it moves between systems and sites.
- ☐ Encryption of information stored on servers, workstations, and mobile devices.
- ☐ How removable media is handled, labeled, transported, and destroyed.
- ☐ How equipment and paper are destroyed at end of life, and what record is kept.

■ The environment

- ☐ Physical security of areas where it is accessed, stored, or printed.
- ☐ Visitor control and escorting in those areas.
- ☐ Screen positioning and whether displays are visible to the public.
- ☐ Network separation between this environment and general office systems.
- ☐ How remote access works, if it exists at all.
- ☐ Mobile and in-vehicle devices, including what happens when one is lost.

■ Watching and responding

- ☐ What is logged, how long logs are kept, and whether anybody reviews them.
- ☐ How malicious software is detected and dealt with.
- ☐ How software updates are applied and verified.
- ☐ Incident detection, reporting, and the timescales your agency is held to.
- ☐ Who must be notified, and how quickly, when something happens.

■ Suppliers and cloud

- ☐ Any cloud or hosted service in the environment, and what it is contractually committed to.
- ☐ Written agreements with anybody who supports or hosts these systems.
- ☐ How vendor access is granted, limited, monitored, and ended.

4 Where the Gaps Usually Are

Not requirements, just the things we most often find undocumented when walking an agency environment for the first time.

Area	What tends to be missing
Scope	Nobody has written down every place the information actually reaches, particularly email, shared folders, and printers.
People who leave	Access is removed from the main system promptly, but not from every system, and rarely on the same day.
Shared logins	One account used by a shift, usually for a piece of equipment or a specialist application.
Documentation	The environment is well understood by one person and written down nowhere.
Vendors	Support arrangements exist and work well, but the written agreements and screening records are hard to locate.
Aging equipment	Machines that still work, still run, and no longer receive security updates.
Logs	Logging is switched on and nobody has ever looked at it.
Backups	Backups exist and have never been restored from, and nobody is sure where they are held.

5 What to Take Into Your Review

Date of our last CJIS audit or review	Findings still outstanding
Next review expected	Who is leading it
Which policy version we are working from	Michigan materials reviewed

■ Notes and priorities



About this worksheet

This document is general planning guidance. It does not establish, certify, or evidence compliance with the FBI CJIS Security Policy, the Michigan Addendum, LEIN policy, or any other requirement, and it is not a substitute for your agency's required review. Requirements change and are determined by the FBI, by Michigan State Police, and by your agency's designated officers. Computer Ties makes no representation that any product, service, or configuration by itself satisfies CJIS requirements. Current source documents are linked from the Computer Ties IT Resource Center. A completed copy of this worksheet describes a criminal justice environment and must be protected accordingly.

Support that understands the environment

Computer Ties works with police departments, fire departments, courts, townships, and municipalities across southern Michigan. We can help you map your environment, document what exists, and address the technology side of findings from a review — working alongside your Terminal Agency Coordinator, Local Agency Security Officer, and state contacts rather than in place of them.

NEW PROJECTS AND PLANNING

(517) 788-6393

EXISTING CUSTOMER SUPPORT

(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990

