



CJIS-Aligned Services

Imperial Valley Info-Tech LLC
Calexico, CA 92231
<https://imperialvalleyinfotech.com>

CJIS-Aligned IT Services for Public Sector & Justice-Adjacent Organizations

Public-sector and justice-adjacent organizations rely on technology environments that must be secure, controlled, and well-documented. Imperial Valley Info-Tech (IVIT) provides CJIS-aligned IT and cybersecurity services designed to support operational integrity, access control, and risk awareness within sensitive environments.

Who We Serve

- Law enforcement and public safety agencies
- Municipal and county departments
- Justice-adjacent organizations and vendors
- Public-sector offices handling sensitive criminal justice information
- Organizations requiring controlled access and documented IT practices

CJIS-Aligned Core Services

Managed IT & Operational Oversight

- Proactive monitoring and maintenance
- Patch and update management
- Structured helpdesk support
- Vendor and service coordination

Result: Stable, predictable IT operations that support mission-critical work.

Cybersecurity & Access Control Awareness

- Enterprise endpoint protection
- Advanced threat detection (EDR)
- Secure DNS and web filtering
- Multi-factor authentication (MFA)
- Administrative access separation

Result: Reduced risk of unauthorized access to sensitive systems and data.

Backup, Recovery & Resilience

- System and data backups
- Ransomware recovery readiness
- Restore testing awareness

Result: Operational continuity following incidents or outages.



Documentation & Environment Visibility

- Network and system documentation
- Asset and access visibility
- Change awareness documentation

Result: Clear understanding of the technology environment supporting justice-related operations.

What to Expect During the Initial IT Evaluation

The Initial IT Evaluation is a structured, non-intrusive review designed to give leadership visibility into the current IT environment without disruption. For CJIS-aligned environments, the evaluation focuses on operational stability, access awareness, and risk identification.

What We Do

- Review the IT environment at a high level
- Discuss workflows, dependencies, and access considerations
- Identify potential risk areas and single points of failure
- Review security and access practices at a high level
- Document observations for leadership review

What We Do Not Do

- We do not install software or agents
- We do not make configuration changes
- We do not interrupt operations
- We do not perform audits or certify CJIS compliance

What You Receive

- A concise findings summary written for leadership
- Clear identification of strengths and risk areas
- Practical next-step considerations, with no obligation
- An executive-friendly overview suitable for internal discussion

Next Steps

Following the Initial IT Evaluation, organizations may choose to:

- Request clarification or follow-up discussion
- Address identified risks internally
- Engage IVIT for ongoing managed or advisory services

To request an Initial IT Evaluation or follow-up discussion, contact IVIT at assessment@imperialvalleyinfotech.com

There is no obligation following the evaluation.

This evaluation is advisory in nature and does not constitute an audit, certification, or validation of CJIS compliance.