

FBI CJIS Security Policy v5.9

The CJIS Security Policy requires security and privacy controls to protect the confidentiality, integrity, and availability of Criminal Justice Information.



What it is

At a glance

PUBLISHER Federal Bureau of Investigation (FBI)	TYPE Framework	VERSION CJIS Security Policy v5.9.3
EFFECTIVE February 2021	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>

Why it matters

- **Strengthen data protection practices** Ensure confidentiality and integrity of criminal justice information through rigorous security and privacy controls tailored to sensitive data.
- **Support regulatory compliance** Enable agencies to meet federal and state legal obligations regarding the handling and safeguarding of criminal justice information.
- **Improve audit readiness** Facilitate consistent documentation, monitoring, and evidence gathering for internal and external audits, reducing compliance risks.
- **Enhance incident response capabilities** Strengthen the organization's ability to detect, report, and recover from security incidents involving criminal justice data.

How SmartSuite supports CJIS Security Policy

CJI Scope and System Boundary

Define where CJI is stored and transmitted with clear boundary documentation.

CJIS Requirement Library

Track CJIS requirements with owners, procedures, and implementation evidence.

Access and Audit Evidence Hub

Centralize user access reviews, authentication proof, and audit logging evidence.

Incident Response and Readiness

Run CJIS-aligned incident workflows with timelines, actions, and lessons learned.

Vendor and Remote Access Oversight

Manage vendor access approvals, monitoring, and supporting evidence.

CJIS Compliance Review and Audit Readiness Reporting

Report readiness, gaps, and evidence coverage for CJIS reviews and audits.

Common framework mappings

FedRAMP Rev. 5

FISMA

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-171 Rev. 3

NIST 800-53 Rev.5

SOC 2

Official resources

CJIS Security Policy

Defines comprehensive cybersecurity and operational controls for protecting Criminal Justice Information (CJI).

le.fbi.gov/cjis-division/cjis-security-policy-resource-center

CJIS Security Policy Resource Center

Provides official documents, updates, and implementation guidance for the CJIS Security Policy.

le.fbi.gov/cjis-division/cjis-security-policy-resource-center

CJIS Security Addendum

Outlines the requirements for private contractors handling Criminal Justice Information.

le.fbi.gov/cjis-division/cjis-security-policy-resource-center/security-addendum

CJIS Security Policy Area 5—Access Control

Describes access control measures specific to the CJIS Security Policy framework.

le.fbi.gov/cjis-division/cjis-security-policy-resource-center/area-5-access-control

Frequently asked questions

What is the CJIS Security Policy used for?

The CJIS Security Policy is designed to protect Criminal Justice Information (CJI) by establishing comprehensive security controls for information systems, personnel, and processes in criminal justice agencies and their partners. It helps ensure confidentiality, integrity, and availability of CJI through prescribed cybersecurity and operational safeguards.

Is compliance with the CJIS Security Policy mandatory?

Yes, compliance with the CJIS Security Policy is mandatory for all agencies and contractors that access or handle CJI, as established by the Federal Bureau of Investigation (FBI). Noncompliance can result in loss of system access or legal consequences.

Who does the CJIS Security Policy apply to?

The CJIS Security Policy applies to federal, state, local, and tribal law enforcement agencies, as well as private contractors and vendors who access, transmit, or store criminal justice information. Any entity interacting with FBI CJIS systems or CJI data falls within its scope.

What are the key security requirements in the CJIS Security Policy?

Organizations must implement controls including user authentication, access control, encryption, network security, personnel vetting, and system monitoring. Requirements also cover incident response, audit logging, physical security, and regular security awareness training.

How should organizations implement the CJIS Security Policy?

Implementation involves integrating the policy's requirements into internal procedures, configuring technical security controls, providing personnel training, and documenting compliance activities. Agencies often develop comprehensive security plans, conduct regular risk assessments, and coordinate with IT and compliance stakeholders.

How does the CJIS Security Policy relate to other cybersecurity frameworks?

While the CJIS Security Policy shares concepts with frameworks like NIST SP 800-53 and ISO 27001, it includes additional requirements specific to the criminal justice sector and CJI protection. Organizations may map CJIS controls to other standards to streamline integrated compliance programs.

What ongoing compliance activities are required by the CJIS Security Policy?

Agencies must continuously maintain and monitor security controls, conduct regular user background checks and security training, and respond to incidents as required by the policy. FBI or authorized agency audits are conducted to verify ongoing compliance, and agencies must retain up-to-date documentation.

How would SmartSuite support CJIS Security Policy?

SmartSuite enables organizations to track CJIS-related risks, manage access control policies, and monitor security controls. It facilitates personnel vetting and security training management, supports evidence documentation for audits, and generates compliance reports to streamline audit readiness and ongoing regulatory oversight.

License included / downloadable: Yes The CJIS Security Policy is published by the FBI CJIS Division and is publicly available through official FBI resources.

Full framework page and mappings: smartsuite.com/frameworks/cjis-security-policy-criminal-justice-information-services-security-policy