

DATA PROTECTION IN TODAY'S WORKPLACE

WHAT YOU NEED TO KNOW

A reference guide to data security and encryption under the CJIS Security Policy

Protection of sensitive data within the workplace has become an increasingly critical issue to our daily operations. Universally the volume and digitization of information has only continued to grow, leading to tremendous amounts of data being created, transmitted and stored every second of every day. To protect the sensitive, highly critical nature of this information the Criminal Justice Information Services Security Policy (CJIS-SP) was established. The following offers a quick reference to the CJIS-SP, data protection mechanisms and general information protection.

What is the Criminal Justice Information Services (CJIS)?

The Criminal Justice Information Services Security Policy (CJIS), established by the FBI, provides a framework for protecting sensitive criminal justice information (CJI) both at rest and in transit. This policy ensures that data remains secure, confidential, and accessible only to authorized personnel.

- **What Data Is Included Within Protection Requirements?**

CJI encompasses a broad range of data, including biometric data (e.g., fingerprints), criminal history records, case files, incident reports, and personally identifiable information (PII) linked to criminal justice activities.

- **Who Does It Apply To?**

The CJIS Security Policy applies to any entity—public or private—that accesses, processes, or stores CJI. This includes law enforcement agencies, courts, prosecutors, contractors/vendors, and non-criminal justice agencies using information for employment purposes.

- **What Is the Intent/Purpose?**

The primary purpose is to safeguard CJI against unauthorized access, use, or disclosure while ensuring its availability for legitimate criminal justice purposes. It aims to standardize security practices across jurisdictions and entities handling sensitive data.

- **Federal and State Oversight/Statutes**

The policy is governed by the FBI's CJIS Division, with compliance enforced under federal statutes like Title 28 CFR Part 20. States may also impose additional regulations through their CJIS Systems Agencies (CSAs), which oversee local implementation and audits.

Sensitive information not covered under CJIS

Even if an organization is not directly bound to comply with CJIS policies, there is an abundance of targeted information which applying the same protections towards would be tremendously beneficial. This includes, but is not limited to:

- PII to include Names/Address/Social Security Numbers
- Protected Health Information (PHI) such as medical records, patient histories, insurance information
- Financial information including credit card numbers, bank account details, credit histories, tax information
- Confidential business information, trade secrets, patient details & proprietary data

Targeting and accessing sensitive information from commercial entities has remained a growing issue with occurrences coming from physical access, insider threat, targeted cyber-attacks, physical media readers and more. An organization exempt from following CJIS does not mean the threat of unauthorized access, and subsequent consequence is any less severe.

Forms of Compliant Protection

To meet CJIS requirements, organizations must implement robust security measures. These can vary between physical and digital solutions, each with specific compliance standards.

- **What are examples of physical data protection?**

Physical data protection involves the safeguarding of tangible devices and information with the intent of preventing unauthorized access, distribution or replication. Common examples include:

- Access control systems: restricting physical access to only authorized personnel
 - Surveillance systems: monitoring activity and alerting unauthorized access
 - Perimeter security: such as physical barriers or guard personnel
 - Locking devices: such as compliant safes with locks for securing physical devices and data
- **What is digital data security?**

Digital data security, or cybersecurity, involves numerous technical, procedural and strategic measures to protect information in its digital state. This would include but not limited to:

- Digital encryption: such as full disk encryption (FDE) or Public Key Infrastructure
- Access control measures based on user roles, passwords and permission groups

- Data loss prevention (DLP) tools to monitor the movement of sensitive information
 - Multifactor authentication adding a second, or multiple forms of verification in addition to password only
 - **Key Terms to Look for in Solutions**

When evaluating security solutions, it is wise to ensure they meet CJIS parameters, even if your organization is not directly governed by CJIS. Two key terms to look for include:

 - *FIPS 140-2 (or Level 3)*: A federal standard for cryptographic modules, ensuring hardware and software meet rigorous security benchmarks. Level 3 adds physical tamper resistance.
 - *128-bit or 256-bit Key Sizes*: Refers to the strength of encryption algorithms (e.g., AES). CJIS mandates at least 128-bit encryption, with 256-bit offering enhanced security for highly sensitive data.
-

"How Does Encryption Work"

Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) using mathematical algorithms and keys. It ensures data confidentiality, even if intercepted.

- **At Rest (Predominantly) and In Transit**
 - *At Rest*: Data stored on devices (e.g., hard drives, servers) is encrypted to prevent unauthorized access if the device is stolen or compromised.
 - *In Transit*: Data moving across networks (e.g., email, cloud uploads) is encrypted to protect against interception. CJIS requires encryption for both states, often using protocols like Transport Layer Security (TLS) for transit.
- **Public Key Infrastructure (PKI) Function (Private Key vs. Public Token)**

Public Key Infrastructure (PKI) uses asymmetric encryption:

 - *Public Key*: Freely shared to encrypt data. Allows any party to encrypt data so that the only person able to access it is the recipient holding the private token.
 - *Private Key*: Kept secret and used to decrypt data.
This dual-key system ensures secure communication and verifies identities via digital certificates.
- **Role of the Cloud vs. HDD Storage**

- *Cloud hosted solutions*: Offer scalability, remote access, and disaster recovery. Requires providers be CJIS compliant with encryption and audit capabilities along with periodic review and/or penetration testing being required to maintain market rating.
- *HDD (Hard Disk Drive)*: Provides local control but is vulnerable to physical damage or theft. Any user of FDE local controls should also have a robust backup and disaster recovery plan commonly requiring additional resources.

Risks of Non-Compliance

Failing to adhere to CJIS Security Policy can result in severe consequences, impacting operations, finances, and personnel.

- **Sanctions**
Agencies or vendors may face fines, penalties, or mandatory corrective actions imposed by federal or state authorities.
- **Loss of Access to CJ**
Non-compliant entities risk losing authorization to access CJ databases (e.g., NCIC), crippling law enforcement functions.
- **Legal Actions/Compensatory Damages**
Data breaches due to non-compliance can lead to lawsuits, with organizations liable for damages to affected individuals or agencies.
- **Loss of Employment**
Individuals responsible for compliance failures may face disciplinary action, including termination, especially if negligence is proven.
- **Additional Risks**
Reputational damage, operational disruptions, and increased scrutiny from regulators further compound the fallout.

Introduction to Biometric Information Management's CHRIsafe Product

For organizations seeking a tailored, CJIS-compliant solution, Biometric Information Management (BIM) offers CHRIsafe—a cutting-edge software platform designed to streamline the management and protection of criminal justice information (CJI) and other sensitive data sets. CHRIsafe integrates advanced encryption (supporting AES 256-bit standards) and secure

data storage both at rest and in transit, meeting or exceeding FIPS 140-2 requirements. The platform supports multi-tiered applications, enabling secure scheduling, background checks, and data encryption within a single, scalable system.

CHRIsafe is particularly valuable for agencies handling biometric data, such as fingerprints, alongside criminal history records. It ensures compliance with CJIS Security Policy by incorporating robust access controls, audit logging, and cloud-compatible architecture—allowing seamless integration with existing infrastructure. Unlike generic solutions, CHRIsafe is customizable to meet the specific needs of any institution reducing vulnerabilities like spoofing or unauthorized access. With its focus on usability and security, CHRIsafe exemplifies how modern technology can address the complexities of CJIS-SP requirements while preparing organizations for future data growth.

Beyond CJIS, CHRIsafe aligns with additional compliance frameworks, enhancing its utility across regulated sectors:

- **NIST 800-53:** CHRIsafe adheres to the National Institute of Standards and Technology's security controls, which underpin federal information systems security and overlap with CJIS requirements. This ensures broader applicability for federal contractors or agencies subject to NIST standards.
- **HIPAA:** For entities handling health-related biometric data (e.g., in forensic healthcare settings), CHRIsafe complies with the Health Insurance Portability and Accountability Act by encrypting protected health information (PHI) and enforcing strict access controls.
- **GDPR:** In scenarios involving international data sharing, CHRIsafe supports the General Data Protection Regulation by offering data residency options and user consent mechanisms, critical for agencies collaborating with European counterparts.
- **FedRAMP:** CHRIsafe's cloud architecture aligns with Federal Risk and Authorization Management Program standards, enabling its use in federal cloud environments with stringent authorization processes.
- **PCI DSS:** For organizations processing payment data alongside CJJ (e.g., in fraud investigations), CHRIsafe meets Payment Card Industry Data Security Standard requirements through encryption and secure key management.

By addressing these additional frameworks, CHRIsafe provides a versatile, future-proof solution that not only satisfies CJIS mandates but also prepares organizations for multi-regulatory compliance, reducing the need for disparate systems and streamlining security management.

Conclusion

The CJIS Security Policy is a critical framework for protecting criminal justice information, requiring a blend of physical and digital security measures. Encryption—whether at rest or in transit—forms the backbone of compliance, with standards like FIPS 140-2 and AES key sizes ensuring robust protection. While initial costs and implementation efforts may seem daunting, the benefits of secure, accessible data far outweigh the risks of non-compliance, which include legal, financial, and operational repercussions. Solutions like Biometric Information Management's CHRIsafe demonstrate how tailored technology can simplify compliance while enhancing security across multiple regulatory landscapes. Organizations must weigh their options carefully, prioritizing scalable, CJIS-compliant solutions to safeguard all forms of sensitive data in an increasingly digital world.