

A COMPREHENSIVE GUIDE TO CJIS COMPLIANCE & IT EXCELLENCE

This guide offers an in-depth look at our robust strategies and innovative practices designed to meet the rigorous standards of CJIS compliance, illustrating our pledge to protect sensitive data & maintain the highest levels of IT service excellence.



ABOUT EATON & ASSOCIATES

Eaton & Associates specializes in full-spectrum IT services, fostering long-term partnerships through strategic IT solutions. Our client portfolio spans governmental, educational, enterprise, SMB, & non-profit sectors, reflecting our adaptability and commitment to IT service excellence.

COMMITMENT TO CJIS COMPLIANCE

We integrate CJIS compliance into the fabric of our service delivery, ensuring rigorous security protocols and responsible data stewardship across all operations for supporting local law enforcement agencies



ONGOING SOC 2 ACCREDITATION

The pursuit of SOC 2 accreditation reinforces our dedication to the highest standards of security and privacy, reflecting our proactive stance in IT governance and risk management. A letter of engagement, and/or a copy of our SOC 2 audit (once completed) can be provided after providing a fully executed NDA document.

COMPREHENSIVE CJIS POLICY AREAS

Navigating the complexities of the Criminal Justice Information Services (CJIS) security policy areas is a cornerstone of our law enforcement IT support operations at Eaton & Associates. Each policy area is meticulously addressed to ensure our practices are not only compliant but also exemplify the highest standards of data protection and cybersecurity. Our comprehensive approach intertwines advanced technology solutions with stringent operational procedures, creating a robust framework that law enforcement agencies can trust for the secure handling of sensitive information.



CJIS compliance is more than a checklist for Eaton & Associates – it is an ongoing commitment to operational excellence and a secure environment. By carefully aligning our IT practices with each of the CJIS policy areas, we safeguard the confidentiality, integrity, and availability of criminal justice information. This alignment ensures that our law enforcement clients can confidently rely on our systems to be secure, resilient, and trustworthy at all times.

Information Exchange Agreements

The exchange of information in a secure and controlled manner is paramount to preserving the integrity of law enforcement operations and protecting sensitive data against breaches.

Our Approach: We implement advanced encryption standards like TLS 1.3 and AES-256 to secure data exchanges. Protocols are verified against federal and state regulations, with third-party validation ensuring CJIS compliance.

Security Awareness Training

Security training empowers personnel to act as a vigilant defense against cyber threats, crucial for the prevention of data compromises that could undermine justice processes.

Our Approach: Eaton & Associates conducts annual, metrics-driven security training via KnowBe4, with simulations that tailor education to evolving threats, ensuring that our team is prepared to uphold CJIS standards.

Incident Response

A swift and decisive reaction to security incidents is crucial for minimizing damage and restoring system integrity, ensuring uninterrupted law enforcement operations.

Our Approach: Our incident response follows an ICS framework, with a PSA/ticketing system categorizing incidents for rapid resolution. We meet or exceed CJIS-mandated SLAs in our response to preserve system and data integrity.

Auditing and Accountability

Detailed tracking and auditing of system activities are vital for identifying potential breaches and providing a forensic trail for investigations.

Our Approach: We employ SIEM tools to aggregate logs, following NIST SP 800-53 audit guidelines for comprehensive reviews, fostering a culture of accountability aligned with CJIS requirements.

Access Control

Restricting data access to authorized individuals is essential to prevent data leaks & unauthorized viewing of sensitive information, maintaining the confidentiality vital to justice and public trust.

Our Approach: Utilizing Role-Based Access Controls (RBAC) and Attribute-Based Access Controls (ABAC), we enforce the principle of least privilege through periodic reviews, ensuring that access is tightly controlled in accordance with CJIS policies.

Identification and Authentication

Robust user verification processes are foundational to ensuring that only legitimate users gain access to sensitive systems and data, forming the front line of defense against unauthorized entry.

Our Approach: Azure AD (Microsoft Entra ID) secures our authentication process, integrating with SAML and OAuth. We enforce MFA, incorporating biometrics and OTPs for a high assurance of user identity.

Configuration Management

Stable and secure system configurations are crucial for operational integrity and reliability, preventing unauthorized alterations that could compromise data security.

Our Approach: Our Configuration Management Database (CMDB), aligned with ITIL standards, maintains system integrity through automated deployment of verified configurations, enabling swift recovery and adherence to CJIS configuration requirements.

Media Protection

Protecting data stored on physical and digital media is essential to prevent unauthorized data access and loss, safeguarding the pillars of information confidentiality and integrity.

Our Approach: Encryption protocols such as SSE-S3 on AWS S3 safeguard our cloud-based media. Access controls and data lifecycle policies are strictly enforced, ensuring CJIS-compliant media protection.

Physical Protection

Securing IT infrastructure from physical threats is a critical aspect of comprehensive data security, supporting the overall protection strategy even in cloud-centric environments.

Our Approach: Biometric systems, surveillance, and intrusion detection secure our physical premises, creating a secure environment that upholds our commitment to CJIS's physical security standards.

Systems and Communications Protection & Information Integrity

Safeguarding system and communication channels against unauthorized access & ensuring data integrity is essential for the protection of information flow within law enforcement agencies.

Our Approach: Next-gen firewalls, deep packet inspection, strict Advanced Threat Protection (ATP) policies on our Microsoft Exchange Online tenant, and SHA-256 for data integrity ensure secure and reliable operations. Regular security assessments validate our adherence to CJIS protocols.

Formal Audits

Structured evaluations of security practices validate adherence to compliance and the effectiveness of security controls, ensuring continuous alignment with CJIS standards.

Our Approach: Our audit processes, guided by SOC II, include internal and external assessments, ensuring ongoing compliance with the evolving landscape of CJIS requirements.

Personal Security

Ensuring the trustworthiness of individuals with data access is fundamental to maintaining a secure CJIS environment, as human factors are critical to overall data security.

Our Approach: Background checks and security clearances are conducted in line with the FBI's NGI program (Live Scans), with periodic reinvestigations to maintain a secure, trusted workforce.

Mobile Devices

Managing the security of mobile devices is essential to mitigate the risks they pose, ensuring that remote access to sensitive data does not become a vector for security breaches.

Our Approach: Stringent Office 365 MDM policies enforce device encryption, Geo-Location tracking, remote wipes, and compliance with automatic quarantining measures for non-compliance, maintaining stringent mobile device security in line with CJIS standards.

CONCLUSION

At Eaton & Associates, we take pride in not only adhering to CJIS compliance but also setting the benchmark for IT security & operational excellence. Our strategies are meticulously crafted, continually evolving to meet and exceed the stringent demands of CJIS compliance and the expectations of our clients.

