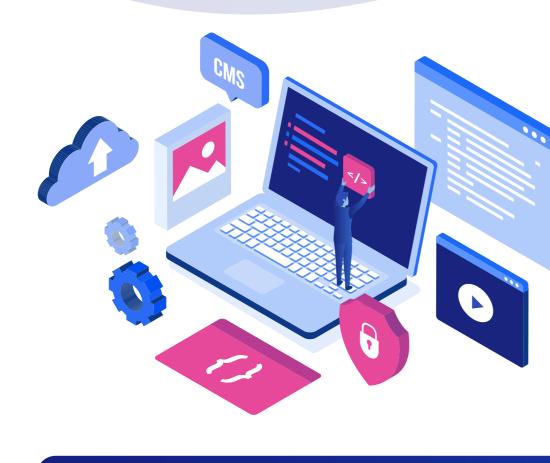
A COMPREHENSIVE GUIDE TO CJIS COMPLIANCE & IT EXCELLENCE

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

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.

Eaton & Associates specializes in full-spectrum

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





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.

Navigating the complexities of the Criminal

COMPREHENSIVE CJIS POLICY AREAS

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, framework that robust creating enforcement agencies can trust for the secure handling of sensitive information.



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

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.

The exchange of information in a secure and controlled manner

is paramount to preserving the integrity of law enforcement





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,



uphold CJIS standards. A swift and decisive reaction to security incidents is crucial

ensuring that our team is prepared to



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

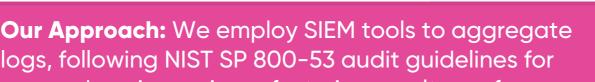
forensic trail for investigations.

system and data integrity.



Auditing and Accountability Detailed tracking and auditing of system activities are vital for identifying potential breaches and providing a

CJIS-mandated SLAs in our response to preserve

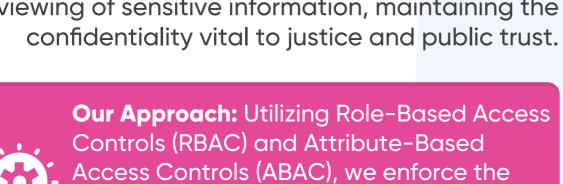


comprehensive reviews, fostering a culture of accountability aligned with CJIS requirements.



Access Control Restricting data access to authorized individuals is essential to prevent data leaks & unauthorized viewing of sensitive information, maintaining the





principle of least privilege through periodic reviews, ensuring that access is tightly controlled in accordance with CJIS policies.



OTPs for a high assurance of user identity.

Our Approach: Azure AD (Microsoft Entra ID) secures

our authentication process, integrating with SAML and

OAuth. We enforce MFA, incorporating biometrics and

Configuration Management







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: Our Configuration Management

adherence to CJIS configuration requirements.

Database (CMDB), aligned with ITIL standards, maintains

Media Protection

system integrity through automated deployment of

verified configurations, enabling swift recovery and



media 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: Encryption protocols

such as SSE-S3 on AWS S3 safeguard

and data lifecycle policies are strictly

enforced, ensuring CJIS-compliant

our cloud-based media. Access controls



creating a secure environment that upholds our commitment to CJIS's physical security standards. **Systems and Communications**

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.

effectiveness of security controls, ensuring

continuous alignment with CJIS standards.

Safeguarding system and communication channels against

unauthorized access & ensuring data integrity is essential for the

Our Approach: Next-gen firewalls, deep packet

inspection, strict Advanced Threat Protection (ATP)

protection of information flow within law enforcement agencies.

Formal Audits Structured evaluations of security practices validate adherence to compliance and the



of CJIS requirements.



maintain a secure, trusted workforce.

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

exceed the stringent demands of CJIS compliance

meticulously crafted, continually evolving to meet and

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





Mobile Devices Managing the security of mobile devices is essential to mitigate the

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 quarantine measures for non-compliance, maintaining stringent mobile device



security in line with CJIS standards.

risks they pose, ensuring that remote access to sensitive data does





and the expectations of our clients.

eatonassoc.com