How to Become CJIS Compliant

Egis IT Security
Shielding Your Business

July 2024 - Written by Susie Johnson

Does your company work with law enforcement agencies? Do you provide software applications, video services or computer hardware to local, state, or federal law enforcement agencies? If so, you may need to become CJIS Compliant.

Criminal Justice Information Services (CJIS) is a division of the FBI that allows access to criminal justice information to local, state, federal and international law enforcement.

The CJIS Security Policy (CSP) provides the controls and security requirements that are necessary to protect criminal justice information (CJI) at all stages of its lifecycle, all the way from the sources of the data to its storage.

Criminal justice information, otherwise known as CJI, is all data that law enforcement may use to perform their duties. The CJIS Security Policy describes types of data that are housed by CJIS: biometric data, identity history data, biographic data, property data, and case/incident history. CJI may be used for criminal investigations, background checks, and various decision-making processes. It is imperative that the data remains confidential and integrous to protect the privacy rights of individuals and to prevent any misuse of the data. The CJIS Security Policy consists of several “policy areas,” which define the measures required to protect CJI. The policy areas are to be examined within each agency or NCJA to determine their applicability. These policy areas are:

- Information Exchange Agreements
- Security Awareness Training
- Incident Response
- Auditing and Accountability
- Access Control
- Identification and Authentication
- Configuration Management
- Media Protection
- Physical Protection
- Systems and Communications Protection and Information Integrity
- Formal Audits
- Mobile Devices

Compliance with the CJIS Security Policy is essential for all organizations and individuals with access to CJIS systems or Criminal Justice Information.

To become CJIS compliant, we recommend doing a gap assessment where we will look for vulnerabilities in your network, review physical building access and your policies and procedures for areas of improvement. We are resellers of many products that you may need to become CJIS compliant including email filtering, anti-virus software, EDR, MDR, Security Awareness Training and monthly vulnerability reporting.

Egis IT Security provides affordable assessments, products, and services. Our team of experts is eager to assist your company in becoming CJIS compliant.

(317) 344-2144 10255 Commerce Dr Suite 250, Carmel, IN 46032 sjohnson@egis-security.com