CJIS

Summary

Regulation: Criminal Justice Information Services

Abbreviation: CJIS

Governs these parties: all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process, or transmit unencrypted CJI

Enforced by: the Criminal Justice Information Services Division

Details

CJIS provides a centralized source of criminal justice data to agencies and authorized third parties throughout the United States. Law enforcement, national security, and intelligence community partners need timely and secure access to services that provide data wherever and whenever for stopping and reducing crime.

CJIS compliance security requirements keep networks aligned when it comes to data security and encryption and ensures that sensitive criminal justice intel is locked down with the continuity of information protection, providing the appropriate controls to protect CJI, from creation through dissemination.

The rest of this document is designed to help our community understand CJIS better by outlining the following information.

- **How it Relates to Cybersecurity**
- **How Coro Handles Compliance for You**

How it Relates to Cybersecurity

Complying with the CJI requires agencies to establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate agency officials and/or authorities.

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system.

Media protection policies and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals.