# Protect Criminal Justice Information and Support CJIS Compliance

Virtru's end-to-end encryption, security settings, granular access controls, and customer-hosted key management capabilities prevent unauthorized access to regulated data.

## CJIS Data Security Requirements

Criminal Justice Information Services (CJIS) analyzes criminal justice information (CJI) from law enforcement centers around the country and provides a centralized database to store and access CJI. To use CJIS databases, organizations must comply with government regulations:

- **Section 5.10.1.2.1** When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption that is FIPS 140-2 certified.
- **Section 5.10.1.2.2** When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption with the same standard mentioned above or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.

Virtru hosts everything in the U.S., uses encryption algorithms that comply with FIPS 140-2, is FedRAMP authorized at the moderate impact level, and adheres to the security controls defined by NIST SP 800-53. Virtru cannot access your protected data at any time.

## Virtru is a Crucial Part of Your Solution to Help Meet CJIS Compliance

### End-to-End Encryption

Protect CJI and any sensitive data you need to share and store with AES-256 bit encryption, FIPS 140-2 compliant modules, and two-factor authentication.

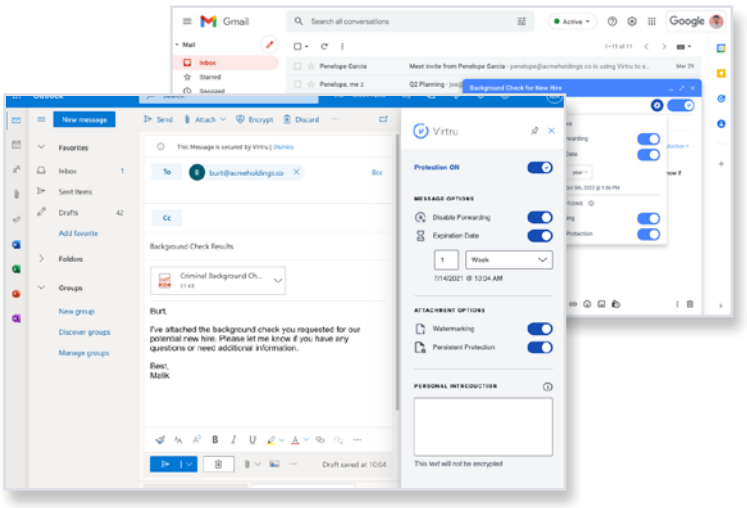
### Encryption Key Management

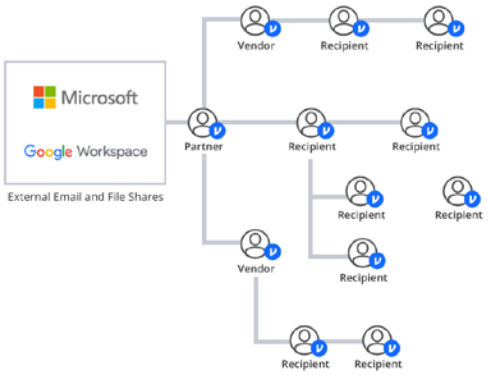
Host your own keys so you never have to trust anyone (including cloud providers) with access to your data. Integrate with existing processes and Hardware Security Modules.

### On-Demand Access Controls

Revoke access and add/adjust access controls at any time. Enable data loss prevention (DLP) rules to identify potential CJI and alert users to add encryption.

# Seamless Data Protection and Control for the Infrastructure, Software, and Devices You Use Today






### Set Encryption Rules & Add Access Controls

Prevent human error by automatically enabling encryption for users who handle CJIS-protected data to protect emails and files. Revoke messages, disable forwarding, set expiration, watermark files, and maintain persistent control of files. Default “encrypt & upload” as the option for users adding documents in Google Drive.

### Support Data Governance Through Granular Audit Trails

View when and where messages and files have been accessed and adapt controls for evolving workflows and collaboration requirements.

## Proven Platform to Support Compliance with Google and Microsoft

### Trusted Data Format

US government approved data protection standard that binds encrypted data to policies and metadata to protect data.

### Software Development Kit (SDK)

Embed data protection and access controls into the apps and systems that power your sensitive, digital workflows.

### Search and E-Discovery

Keep messages searchable and exportable for Freedom of Information Act requests, audits, or other e-discovery requirements.

## Trusted by State and Local Governments, Federal Agencies, and Thousands of Other Organizations.

Maryland

City of Evanston

virtru

Learn how Virtru helps you meet CJIS compliance and supports your organizational goals for data protection: **virtru.com/contact-us**