The CJIS Security Policy

To protect criminal justice information, the FBI created the CJIS Security Policy document – that defines implementation requirements and standards for the following 13 security policy areas:

1. **Information exchange agreements**
   The CJIS Security Policy includes procedures for how the information is handled and what should be in user agreements. Companies and agencies that use criminal justice information must include specific processes and parameters in their information exchange agreements, including:
   - Audits
   - Logging
   - Quality assurance
   - Pre-employment screening
   - Security
   - Timeliness
   - Training
   - Use of systems
2. **Security awareness training**
   Anyone with access to criminal justice information must undergo security awareness training within six months of receiving the information. The training must be repeated every two years to meet CJIS compliance standards. Individual training and topics covered are based on the access and interaction the individual has to the criminal justice data.
3. **Incident response**
   To meet CJIS compliance, all breaches and major incidents need to be reported to the Justice Department. Companies and agencies must establish procedures for detection, analysis, containment, recovery, and user responses for all breaches and incidents.
4. **Auditing and accountability**
   The following events must be audited:
   - Login attempts
   - Assessments, creation, or changing/editing of permissions on user accounts, files, directories, and other system resources
   - Attempts to modify passwords
   - Actions by privileged accounts
   - Attempts to access, modify, or destroy history/log files
5. **Access control**
   Users who have access to criminal justice information and the types/levels of access must be identified, monitored, and tracked. Least privileged access should be enforced when necessary to reduce risk to the information. Access control criteria should be given on a need-to-know/need-to-share basis and provided based on job, location, network address, and/or time restrictions.
6. **Identification and authentication**
   Each person who is authorized to use CJIS must have unique identification and a standard authentication method such as a password, token or PIN, biometrics, or another type of multi-factor authentication.

7. **Configuration management**
   Whether planned or unplanned, changes and updates to the information system platform, architecture, hardware, software, and procedures must be documented. That documentation must be protected from unauthorized access.
8. **Media protection**
   You must have policies and procedures documented for how digital and physical media will be securely stored, accessed, transported, and destroyed.
9. **Physical protection**
   Physical media (documents or digital media storage devices) needs to be handled securely. Access to physical media needs to be limited and monitored.
10. **Systems and communications protection and information integrity**
    Applications, services, and information systems must ensure data security and system and network integrity. This includes defining and enforcing where and how information can travel within and between systems.
11. **Formal audits**
    The FBI and other agencies may conduct formal audits to ensure CJIS compliance.
12. **Personnel security**
    Anyone that will have access to unencrypted CJIS data must go through detailed security screening during hiring, termination, transfer, and other employees or third-party vendor lifecycle events.
13. **Mobile devices**
    The CJIS policy outlines considerations and requirements for managing systems and network access via smartphones, tablets, and other mobile devices. This includes using wireless security protocols such as WEP and WPA, device certificates, etc.