5.8 Media Protection (MP) Policy

PURPOSE

Documented and implemented media protection policies and procedures ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes. The organization may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

This policy applies to any digital and/or non-digital media containing MI/FBI criminal justice information (CJI) while being stored, accessed, or physically moved from a secure location from the [*agency name*]. This policy applies to any authorized person who accesses, stores, and/or transports digital or non-digital media. Transporting CJI outside the agency’s assigned physically secure area must be monitored and controlled. Authorized [*agency name*] personnel shall protect and control digital or non-digital CJI while at rest and in transit. The [*agency name*] will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the [*agency name*] operational personnel with security responsibilities (LASO) and/or Terminal Agency Coordinator (TAC). Procedures shall be defined to facilitate the implementation of the media protection policy and the associated media protection controls including reviewing and updating the media protection policy and procedures at least annually and following any security incidents involving digital and/or non-digital media.

POLICY

01. MEDIA ACCESS

1. The [*agency name*] shall restrict access to digital and/or non-digital media to authorized individuals.

02. MEDIA STORAGE

1. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on agencies, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

The [*agency name*] shall:

1. Physically control and securely store digital and non-digital media within the physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible.
2. Protect system media types until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

03. MEDIA TRANSPORT

1. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel. Agencies establish documentation requirements for activities associated with the transport of system media in accordance with agency assessments of risk. Agencies maintain the flexibility to define recordkeeping methods for the different types of media transport as part of a system of transport-related records.
2. The [*agency name*] shall:
3. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel. .
4. Maintain accountability for system media during transport outside of the physically secure location or controlled areas.
5. Document activities associated with the transport of information system media.
6. Restrict the activities associated with the transport of information system media to authorized personnel.

04. MEDIA SANITIZATION

1. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, deidentification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Agencies determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.
2. The [*agency name*] shall:
   1. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposed, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.
   2. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

05. MEDIA USE

1. The [*agency name*] shall:
2. Restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of CJI by using technical, physical, or administrative controls.
3. Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CJI.
4. Prohibit the use of media devices on all agency owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.

PROCEDURES

Agency must provide the procedures on how the policies will be implemented.

COMPLIANCE

Agencies are required to review and update the current incident response policy and procedure annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE

AC-19, AC-20, PL-4.