

Policy Name:	Media Protection
Policy Number:	37
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.8 Media Protection (MP)

PURPOSE

To ensure that Information Technology (IT) controls access to and disposes of media resources in compliance with **Westbrook Police Department** security policies, standards, and procedures.

POLICY

This policy is applicable to all departments and users of IT resources and assets of **Westbrook Police Department**.

1. MEDIA ACCESS:

IT through direction from **Westbrook Police Department** shall:

- a. Restrict access to digital and non-digital media to authorized individuals.
- b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. MEDIA STORAGE

The **Westbrook Police Department** shall:

- a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible.
- b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT

The **Westbrook Police Department** shall:

- a. 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, as defined in SC-13 and SC-28 of this Policy. 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.

- b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas.
- c. Document activities associated with the transport of system media.
- d. Restrict the activities associated with the transport of system media to authorized personnel.

4. MEDIA SANITIZATION

The **Westbrook Police Department** shall:

- a. 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 purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.
- a. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5. MEDIA USE

The **Westbrook Police Department** shall:

- a. Restrict the use of digital and non-digital media on **Westbrook Police Department** owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls.
- b. Prohibit the use of personally owned digital media devices on all **Westbrook Police Department** owned or controlled systems that store, process, or transmit criminal justice information.
- c. Prohibit the use of digital media devices on all **Westbrook Police Department** owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

ROLES AND RESPONSIBILITIES:

Local Agency Security Officer: Ensure that policies and procedures required by the FBI CJIS Security Policy are developed and maintained. Ensure that policies and procedures are disseminated and operationalized.

Westbrook Police Department Information Technology Staff: Develop, document, and disseminate to authorized individuals:

Agency-level media protection policy that:

- (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

Procedures to facilitate the implementation of the media protection policy and the associated media protection controls.

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures.

Review and update the current media protection:

1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.
2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.

Westbrook Police Department Personnel: All **Westbrook Police Department** personnel will understand what constitutes media protection.

COMPLIANCE:

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:

National Institute of Standards and Technology (NIST)
FBI CJIS Security Policy

CLEO or Agency Director

Date Issued:	08/11/2026
Date Reviewed:	08/11/2026