

Policy Name:	Systems and Communications Protection
Policy Number:	31
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.10 Systems and Communications Protection (SC)

PURPOSE:

To establish guidelines for system and communications protection for Information Technology (IT) resources and information systems for Westbrook Police Department.

POLICY:

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

1. APPLICATION PARTITIONING

The Westbrook Police Department shall:

- a. Separate user functionality, including user interface services, from system management functionality.

2. INFORMATION IN SHARED RESOURCES

The Westbrook Police Department shall:

- a. Prevent unauthorized and unintended information transfer via shared system resources.

3. DENIAL OF SERVICE PROTECTION

The Westbrook Police Department shall:

- a. Protect against or limit the effects of the following types of denial of service events: Distributed Denial of Service, DNS Denial of Service, etc.
- b. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.

4. BOUNDARY PROTECTION

The Westbrook Police Department shall:

- a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
- b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks.
- c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
- d. Limit the number of external network connections to the system.
- e. Implement a managed interface for each external telecommunication service.
- f. Establish a traffic flow policy for each managed interface.
- g. Protect the confidentiality and integrity of the information being transmitted across each interface.
- h. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.
- i. Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need.
- j. Prevent unauthorized exchange of control plane traffic with external networks.
- k. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.
- l. Filter unauthorized control plane traffic from external networks.
- m. Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJJ.
- n. Prevent split tunneling for remote devices connecting to Westbrook Police Department systems.
- o. Route all internal communications traffic that may be proxied, except traffic specifically exempted by Westbrook Police Department personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.
- p. For systems that process personally identifiable information:
 - i. Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
 - ii. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system.
 - iii. Document each processing exception.
 - iv. Review and remove exceptions that are no longer supported.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY

The Westbrook Police Department shall:

- a. Protect the confidentiality and integrity of transmitted information.
- b. Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJJ during transmission.

6. NETWORK DISCONNECT

The Westbrook Police Department shall:

- a. Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

The **Westbrook Police Department** shall:

- a. Establish and manage cryptographic keys for required cryptography employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by Westbrook Police Department

8. CRYPTOGRAPHIC PROTECTION

The **Westbrook Police Department** shall:

- a. Determine the use of encryption for CJI in-transit when outside a physically secure location.
- b. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.

9. COLLABORATIVE COMPUTING DEVICES

The **Westbrook Police Department** shall:

- a. Prohibit remote activation of collaborative computing devices and applications.
- b. Provide an explicit indication of use to users physically present at the devices.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES

The **Westbrook Police Department** shall:

- a. Issue public key certificates under an agency-level certificate for obtain public key certificates from an approved service provider.
- b. Include only approved trust anchors in trust stores or certificate stores managed by **[insert agency name]**.

11. MOBILE CODE

The **Westbrook Police Department** shall:

- a. Define acceptable and unacceptable mobile code and mobile code technologies.
- b. Authorize, monitor, and control the use of mobile code within the information system.

12. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

The **Westbrook Police Department** shall:

- a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
- b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

13. SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

The **Westbrook Police Department** shall:

- a. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

14. ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

The **Westbrook Police Department** shall:

- a. Ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

15. SESSION AUTHENTICITY

The **Westbrook Police Department** shall:

- a. Protect the authenticity of communications sessions.

16. PROTECTION OF INFORMATION AT REST

The **Westbrook Police Department** shall:

- a. Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength. Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity. The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States—federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).
- b. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.

17. PROCESS ISOLATION

The **Westbrook Police Department** shall:

- a. Maintain a separate execution domain for each executing system process.

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 organizational personnel with system and communications protection responsibilities:

Agency-level system and communications 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 system and communications protection policy and the associated system and communications protection controls.

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures.

Review and update the current system and communications protection:

- 1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and
- 2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.

Westbrook Police Department Personnel: All **Westbrook Police Department** personnel will understand what constitutes system and communications 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) Special Publications (SP)
FBI CJIS Security Policy

CLEO or Agency Director

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

SAMPLE