

Policy Name:	Configuration Management
Policy Number:	43
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.7 Configuration Management (CM)

PURPOSE:

To ensure that Information Technology (IT) resources are inventoried and configured in compliance with IT security policies, standards, and procedures.

POLICY:

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

a. BASELINE CONFIGURATION

The **Westbrook Police Department** shall:

- a. Develop, document, and maintain under configuration control, a current baseline configuration of the system.
- b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services
- c. Review and update the baseline configuration and topological drawing of the system:
 - a. At least annually
 - b. When required due to security-relevant changes to the system and/or security incidents occur; and
 - c. When system components are installed or upgraded.
- d. Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.
- e. Retain at least one (1) previous version of baseline configurations of the system to support rollback.

- f. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk.
 - g. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional.
- b. CONFIGURATION CHANGE CONTROL
The **Westbrook Police Department** shall:
 - a. Determine the types of changes to the system that are configuration-controlled.
 - b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.
 - c. Document configuration change decisions associated with the system.
 - d. Implement approved configuration-controlled changes to the system.
 - e. Retain records of configuration-controlled changes to the system for two (2) years.
 - f. Monitor and review activities associated with configuration-controlled changes to the system.
 - g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.
 - h. Test, validate, and document changes to the system before finalizing the implementation of the changes.
 - i. Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.
- c. IMPACT ANALYSIS
The **Westbrook Police Department** shall:

- a. Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
- b. After-system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.
- d. ACCESS RESTRICTIONS FOR CHANGE
The **Westbrook Police Department** shall:
 - a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
- e. CONFIGURATION SETTINGS
The **Westbrook Police Department** shall:
 - a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards.
 - b. Implement the configuration settings.
 - c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements.
 - d. Monitor and control changes to the configuration settings in accordance with **Westbrook Police Department** policies and procedures.
- f. LEAST FUNCTIONALITY
The **Westbrook Police Department** shall:
 - a. Configure the system to provide only essential capabilities to meet **Westbrook Police Department** requirements.
 - b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required.
 - c. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services.

- d. Disable functions, ports, protocols, and services within the system deemed to be unnecessary and/or insecure.
- e. Prevent program execution in accordance with rules of behavior and/or rules authorizing the terms and conditions of software program usage.
- f. Identify software programs authorized to execute on systems.
- g. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.
- h. Review and update the list of authorized software programs annually.
- g. SYSTEM COMPONENT INVENTORY
The **Westbrook Police Department** shall:
 - a. Develop and document an inventory of system components that:
 - i. Accurately reflects the system.
 - ii. Includes all components within the system.
 - iii. Does not include duplicate accounting of components or components assigned to any other system.
 - iv. Is at the level of granularity deemed necessary for tracking and reporting.
 - v. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location
 - b. Review and update the information system component inventory annually.
 - c. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly.
 - d. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.

h. CONFIGURATION MANAGEMENT PLAN

IT shall develop, document, and implement a configuration management plan for the **Westbrook Police Department** system that:

- a. Addresses roles, responsibilities, and configuration management processes and procedures.
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
- c. Defines the configuration items for the information system and places the configuration items under configuration management.
- d. Is reviewed and approved by **Westbrook Police Department** personnel with information security responsibilities and **Westbrook Police Department** personnel with configuration management responsibilities
- e. Protects the configuration management plan from unauthorized disclosure and modification.

i. SOFTWARE USAGE RESTRICTIONS

The **Westbrook Police Department** shall:

- a. Use software and associated documentation in accordance with contract agreements and copyright laws.
- b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
- c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

j. USER-INSTALLED SOFTWARE

The **Westbrook Police Department** shall:

- a. Establish agency-level policies governing the installation of software by users.
- b. Enforce software installation policies through automated methods.
- c. Monitor policy compliance through automated methods at least weekly.

k. INFORMATION LOCATION

The **Westbrook Police Department** shall:

- a. Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted;
- b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
- c. Document changes to the location (i.e., system or system components) where the information is processed and stored.
- d. Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy

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