

Policy Name:	Planning
Policy Number:	39
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.17 Planning (PL)

PURPOSE:

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

POLICY:

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

1. SYSTEM SECURITY AND PRIVACY PLANS

The **Westbrook Police Department** shall:

- a. Develop a security and privacy plans for the system that:
 - i. Are consistent with **Westbrook Police Department** enterprise architecture.
 - ii. Explicitly define the constituent system components.
 - iii. Describe the operational context of the system in terms of missions and business processes.
 - iv. Identify the individuals that fulfill system roles and responsibilities.
 - v. Identify the information types processed, stored, and transmitted by the system
 - vi. Describe any specific threats to the system that are of concern to **Westbrook Police Department**.
 - vii. Provide the results of a privacy risk assessment for systems processing personally identifiable information.
 - viii. Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
 - ix. Provide an overview of the security and privacy requirements for the system.
 - x. Identify any relevant control baselines or overlays, if applicable.

- xii. Include risk determinations for security and privacy architecture and design decisions.
 - xiii. Include security- and privacy-related activities affecting the system that require planning and coordination with **Westbrook Police Department** personnel with system security and privacy planning and plan implementation responsibilities; system developers; **Westbrook Police Department** personnel with information security and privacy responsibilities.
 - xiv. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
 - b. Distribute copies of the plans and communicate subsequent changes to the plans to **Westbrook Police Department** personnel with system security and privacy planning and plan implementation responsibilities; system developers; **Westbrook Police Department** personnel with information security and privacy responsibilities.
 - c. Review the security plan for the information system at least annually or when required due to system changes or modifications.
 - d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.
 - e. Protect the plans from unauthorized disclosure and modification.
2. RULES OF BEHAVIOR
- The **Westbrook Police Department** shall:
- a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
 - b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.
 - c. Review and update the rules of behavior at least annually.
 - d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.
 - e. Include in the rules of behavior, restrictions on:
 - i. Use of social media, social networking sites, and external sites/applications.

- ii. Posting organizational information on public websites.
- iii. Use of **Westbrook Police Department** -provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

3. SECURITY AND PRIVACY ARCHITECTURE

The **Westbrook Police Department** shall:

- a. Develop security and privacy architectures for the system that:
 - i. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.
 - ii. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
 - iii. Describe how the architectures are integrated into and support the enterprise architecture.
 - iv. Describe any assumptions about, and dependencies on, external systems and services
- b. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture.
- c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

4. CENTRAL MANAGEMENT

The **Westbrook Police Department** shall:

- a. The CJISSECPOL is centrally managed by the FBI CJIS ISO.

5. BASELINE SELECTION

The **Westbrook Police Department** shall:

- a. Select a control baseline for the system.

6. BASELINE TAILORING

The **Westbrook Police Department** shall:

- a. Tailor the selected control baseline by applying specified tailoring actions

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 planning responsibilities:

Agency-level planning 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 planning policy and the associated planning controls.

Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures.

Review and update the current planning:

- 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 planning.

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