Policy Name:	Risk Assessment
Policy Number:	40
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.19 Risk Assessment (RA)

PURPOSE:

_____

To ensure that Information Technology (IT) performs risk assessments 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**.

1. SECURITY CATEGORIZATION
   The **Westbrook Police Department** shall:

   a. Categorize the system and information it processes, stores, and transmits.
   b. Document the security categorization results, including supporting rationale, in the security plan for the system.
   c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

2. RISK ASSESSMENT
   The **Westbrook Police Department** shall:

   a. Conduct a risk assessment, including:
      i. Identifying threats to and vulnerabilities in the system.
      ii. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information.
      iii. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

   b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.

   c. Document risk assessment results in a risk assessment report.

   d. Review risk assessment results at least quarterly.

e. Disseminate risk assessment results to **Westbrook Police Department** personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities.

f. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

3. VULNERABILITY MONITORING AND SCANNING
The **Westbrook Police Department** shall:

a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported.

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

i. Enumerating platforms, software flaws, and improper configurations.

ii. Formatting checklists and test procedures.

iii. Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from vulnerability monitoring.

d. Remediate legitimate vulnerabilities within the number of days listed:

i. Critical-7 days
ii. High-30 days
iii. Medium-60 days
iv. Low-90 days

e. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems.

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

g. Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.

h. Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.

i. Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

4. RISK RESPONSE
   The **Westbrook Police Department** shall:

   a. Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

5. CRITICALITY ANALYSIS
   The **Westbrook Police Department** shall:

   a. Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

ROLES AND RESPONSIBLITIES:
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 risk assessment responsibilities:

Agency-level risk assessment 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 risk assessment policy and the associated risk assessment controls.

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

Review and update the current risk assessment:

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 risk assessment.

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
BCA CJDN Security Policy

_____

CLEO or Agency Director

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