Policy Name:	System and Information Integrity
Policy Number:	38
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.15 System and Information Integrity (SI)

PURPOSE:

To ensure that Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

POLICY:

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

1. FLAW REMEDIATION
   The **Westbrook Police Department** shall:

   a. Identify, report, and correct information system flaws.

   b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

   c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;
   - Critical – 7 days
   - High – 30 days
   - Medium – 60 days
   - Low – 90 days

   d. Incorporate flaw remediation into the configuration management process.

   e. Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

2. MALICIOUS CODE PROTECTION
   The **Westbrook Police Department** shall:

   a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with **Westbrook Police Department** configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

   i. Perform periodic scans of the information system at least daily and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the **Westbrook Police Department** policy.

   ii. Block malicious code; quarantine malicious code; send alert to administrator and/or organizational personnel with information security responsibilities in response to malicious code detection.

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

3. SYSTEM MONITORING
   The **Westbrook Police Department** shall:

   a. Monitor the information system to detect:

      i. Attacks and indicators of potential attacks.
         a. Intrusion detection and prevention
         b. Malicious code protection
         c. Vulnerability scanning
         d. Audit record monitoring
         e. Network monitoring
         f. Firewall monitoring

      ii. Unauthorized local, network, and remote connections.

   b. Identify unauthorized use of the information system through defined techniques and methods: event logging.

   c. Invoke internal monitoring capabilities or deploy monitoring devices.

      a. Strategically within the system to collect **Westbrook Police Department** - determined essential information.
      b. At ad hoc locations within the system to track specific types of transactions of interest to the **Westbrook Police Department**.

   d. Analyze detected events and anomalies.

   e. Adjust the level of system monitoring activity when there is a change in risk to **Westbrook Police Department** operations and assets, individuals, other organizations, or the Nation.

f. Obtain legal opinion regarding system monitoring activities.

g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to **Westbrook Police Department** personnel with information security responsibilities weekly.

h. Employ automated tools and mechanisms to support near real-time analysis of events.

i. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.

j. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within **Westbrook Police Department** systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.

k. Alert **Westbrook Police Department** personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications

4. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
The **Westbrook Police Department** shall:

a. Receive information system security alerts, advisories, and directives from **[insert source name]** on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as deemed necessary.

c. Disseminate security alerts, advisories, and directives to: **Westbrook Police Department** personnel implementing, operating, maintaining, and using the system.

d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

5. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
The **Westbrook Police Department** shall:

a. Employ integrity verification tools to detect unauthorized changes to agency software, firmware, and information systems that contain or process CJI.

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

c. Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.

d. Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

6. SPAM PROTECTION
The **Westbrook Police Department** shall:

a. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages.

b. Update spam protection mechanisms when new releases are available in accordance with the **Westbrook Police Department** configuration management policy and procedures.

c. Automatically update spam protection mechanisms at least daily.

7. INFORMATION INPUT VALIDATION
The **Westbrook Police Department** shall:

a. Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

8. ERROR HANDLING
The **Westbrook Police Department** shall:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

b. Reveal error messages only to organizational personnel with information security responsibilities.

9. INFORMATION MANAGEMENT AND RETENTION
The **Westbrook Police Department** shall:

a. Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

b. Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected.

c. Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.

d. Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.

10. MEMORY PROTECTION
The **Westbrook Police Department** shall:

a. Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.

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 all organizational personnel with system and information integrity responsibilities and information system owners:

Agency-level system and information integrity 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 information integrity policy and the associated system and information integrity controls.

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

Review and update the current system and information integrity:

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 system and information integrity.

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
BCA CJDN Security Policy

_____

CLEO or Agency Director

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