Policy Name:	Incident Response
Policy Number:	41
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.3 Incident Response (IR)

PURPOSE:

To ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

POLICY:

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

1. INCIDENT RESPONSE TRAINING
   The **Westbrook Police Department** shall:

   a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

      i. Prior to assuming an incident response role or responsibility or acquiring system access.

      ii. When required by information system changes.

      iii. Annually thereafter.

   b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

   c. Provide incident response training on how to identify and respond to a breach, including the **Westbrook Police Department** process for reporting a breach.

2. INCIDENT RESPONSE TESTING
   The **Lamberton Police Department** shall:

   a. Test the effectiveness of the incident response capability for the information system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.

      a. Coordinate incident response testing with **Westbrook Police Department** elements responsible for related plans.

3. INCIDENT HANDLING
   The **Westbrook Police Department** shall:

   a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

   b. Coordinate incident handling activities with contingency planning activities.

   c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

   d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

   e. Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

4. INCIDENT MONITORING
5. The **Westbrook Police Department** shall:

   a. Track and document incidents.

6. INCIDENT REPORTING
   The **Westbrook Police Department** shall:

   a. Require personnel to report suspected incidents to **Westbrook Police Department** incident response capability within immediately but not to exceed one (1) hour after discovery.

   b. Report incident information to **Westbrook Police Department** personnel with incident handling responsibilities, and if confirmed, notify the BCA Information Security Office (ISO) within 24 hours of discovery.

   c. Report incidents using automated mechanisms.

   d. Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

7. INCIDENT RESPONSE ASSISTANCE
   The **Westbrook Police Department** shall:

a. Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
b. Increase the availability of incident response information and support using automated mechanisms described in the discussion

8. INCIDENT RESPONSE PLAN
The **Westbrook Police Department** shall:

a. Develop an incident response plan that:

i. Provides **Westbrook Police Department** with a roadmap for implementing its incident response capability.

ii. Describes the structure and organization of the incident response capability.

iii. Provides a high-level approach for how the incident response capability fits into the overall **Westbrook Police Department**.

iv. Meets the unique requirements of the **Westbrook Police Department**, which relate to mission, size, structure, and functions.

v. Defines reportable incidents.

vi. Provides metrics for measuring the incident response capability within the **Westbrook Police Department**.

vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

viii. Addresses the sharing of incident information.

ix. Is reviewed and approved by **Westbrook Police Department** annually.

b. Distribute copies of the incident response plan to **Westbrook Police Department** personnel with incident handling responsibilities.

c. Update the incident response plan to address system changes and organizational changes or problems encountered during plan implementation, execution, or testing.

d. Communicate incident response plan changes to **Westbrook Police Department** personnel with incident handling responsibilities.

e. Protect the incident response plan from unauthorized disclosure and modification.

f. Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.

b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.

c. Identification of applicable privacy requirements.

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 personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:

Agency-level incident response 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 incident response policy and the associated incident response controls.

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures.

Review and update the current incident response:

1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Westbrook Police Department Personnel: All **Westbrook Police Department** personnel will understand what constitutes incident response.

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