

Policy Name:	Auditing and Accountability
Policy Number:	35
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.4 Audit and Accountability (AU)

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 for **Westbrook Police Department**.

1. EVENT LOGGING

The **Westbrook Police Department** shall:

- a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III).
- b. Coordinate the security audit function with other **Westbrook Police Department** entities requiring audit.
- c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
- d. Determine that the following events are to be audited within the information system:
 1. *System log-on attempts*
 2. *Attempts to use:*
 - a. *Access permission on a user account, file, directory, or other system resource;*
 - b. *Create permission on a user account, file, directory, or other system resource;*
 - c. *Write permission on a user account, file, directory, or other system resource;*
 - d. *Delete permission on a user account, file, directory, or other system resource;*
 - e. *Change permission on a user account, file, directory, or other system resource.*
 3. *Attempts to change account passwords*
 4. *Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)*
 5. *Attempts for users to:*
 - a. *Access the audit log file;*
 - b. *Modify the audit log file;*
 - c. *Destroy the audit log file.*

2. CONTENT OF AUDIT RECORDS

The **Westbrook Police Department** shall:

- a. Ensure that audit records contain information that establishes the following:
 - a. What type of event occurred.
 - b. When the event occurred.
 - c. Where the event occurred.
 - d. Source of the event.
 - e. Outcome of the event.
 - f. Identity of any individuals, subjects, or objects/entities associated with the event.
- b. Generate audit records containing the following additional information:
 - a. Session, connection, transaction, and activity duration;
 - b. Source and destination addresses;
 - c. Object or filename involved; and
 - d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
 - e. The III portion of the log shall clearly identify:
 1. The operator
 2. The authorized receiving agency
 3. The requestor
 4. The secondary recipient
- c. Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected.

3. AUDIT STORAGE CAPACITY

The **Westbrook Police Department** shall:

- a. Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.

4. RESPONSE TO AUDIT PROCESSING FAILURES

The **Westbrook Police Department** shall:

- a. Alert **Westbrook Police Department** personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure.
- b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.

5. AUDIT REVIEW, ANALYSIS, AND REPORTING

The **Westbrook Police Department** shall:

- a. Review and analyze information system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
- b. Report findings to **Westbrook Police Department** personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities.
- c. Integrate audit record review, analysis, and reporting processes using automated mechanisms.
- d. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

6. AUDIT RECORD REDUCTION AND REPORT GENERATION

The **Westbrook Police Department** shall:

- a. Provide an audit reduction and report generation capability that:
 - i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.
 - ii. Does not alter the original content or time ordering of audit records.
- b. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.

7. TIME STAMPS

The **Westbrook Police Department** shall:

- a. Use internal system clocks to generate time stamps for audit records.
- b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) or that include the local time offset as part of the time stamp.

8. PROTECTION OF AUDIT INFORMATION

The **Westbrook Police Department** shall:

- a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.

- c. Authorize access to management of audit logging functionality to only **Westbrook Police Department** personnel with audit and accountability responsibilities, **Westbrook Police Department** personnel with information security and privacy responsibilities, and system/network administrators.

9. AUDIT RECORD RETENTION

The **Westbrook Police Department** shall:

- a. Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

10. AUDIT GENERATION

The **Westbrook Police Department** shall:

- a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs.
- b. Allow **Westbrook Police Department** personnel with audit record generation responsibilities, **Westbrook Police Department** personnel with information security and privacy responsibilities, and system/network administrators to select which auditable events are to be audited by specific components of the information system.
- c. Generate audit records for the events with the content as defined in AU-2c that include the audit record content defined in AU-3.

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 audit and accountability responsibilities:

Agency-level and system-level audit and accountability 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 audit and accountability policy and the associated audit and accountability controls.

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

Review and update the current audit and accountability:

- 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 audit and accountability.

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

CLEO or Agency Director

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