



Audit Policy

Policy Title: Audit
Policy Number: OLLEISN-004
Policy Date: 01/14/2005

Effective Date: 10/12/2004

1.0 Purpose of Policy

The purpose of this policy is to establish audit requirements for the Ohio Local Law Enforcement Information-Sharing Network central database.

2.0 Scope of Policy

The scope of this policy includes all sworn law enforcement officers and non-sworn civilian law enforcement employees who are granted access to the Ohio Local Law Enforcement Information-Sharing Network by their agency Chief Executive Officer (CEO).

3.0 Background

The purpose of the Ohio Local Law Enforcement Information-Sharing Network is to provide Ohio's law enforcement community with the information necessary to prevent and respond to acts of terrorism and crime. To ensure the timeliness and completeness of the information submitted to the database, the system will be audited periodically. A participating agency CEO may request an audit of an employee's use of the Network.

4.0 References and Authority

4.1 A glossary of terms or acronyms found in this policy is located in Section 6.0 of this policy. The first occurrence of a defined term or acronym is ***bold italicized***.

5.0 Policy

This policy establishes guidelines regarding audits of information housed in the central database of the Ohio Local Law Enforcement Information-Sharing Network (hereafter referred to as the "Network").

5.1 The Network database will be audited periodically by the designated OHLEG network administrators to ensure: the timeliness and completeness of information submitted according to each agency's participation agreement; the security of the system; to investigate potential inappropriate uses of the system; and to identify training needs.

5.2 The Network central database will include an audit capability to log user actions, including the date and time of transaction, individual requesting the transaction, and type of transaction.

5.2.1 The **audit log** of individual user transactions submitted to the Network's central database will be maintained for one year from the date a transaction is initiated.

5.3 Multi-agency providers with an **Originating Agency Identifier** (ORI) must secure a password from the OHLEG Administrator to utilize a single sign-on access for OLLEISN participants.

5.3.1 If the OHLEG Administrator issues the multi-agency provider a password for single sign-on access, the multi-agency provider shall submit the OHLEG User ID and the participating agency's ORI for each transaction submitted to the OLLEISN system.

5.4 Local Law Enforcement Audit Requests. An agency CEO may request an audit of network usage by any of his/her employees.

5.4.1 A request for an audit must state the purpose for the audit and be placed in writing by the agency CEO.

5.4.2 All audit requests will be directed to the designated OHLEG Network Administrator.

5.4.3 The designated OHLEG Network Administrator will copy the OLLEISN Administrative Head on requests for audits.

5.4.4 The agency CEO shall provide the OLLEISN Administrative Head written notice of his/her final disposition of the audit request within 30 days of receiving the audit.

5.4.5 The OLLEISN Administrative Head will immediately notify the Chair of the OLLEISN Steering Committee of any potential misuse of the Network.

5.4.6 The OLLEISN Steering Committee will review and determine any necessary actions regarding misuse of the Network.

6.0 Definitions

6.1 Audit Log: The official report of network transactions.

6.2 Originating Agency Identifier. A unique 9 character number assigned to each law enforcement agency by the National Crime Information Center (NCIC).

7.0 Revision History

<i>Date</i>	<i>Change</i>
10/12/2004	Original policy.
12/16/2004	Section 5.3 added to policy per November 19, 2004 OLLEISN Steering Committee recommendation to allow multi-agency providers to use a single sign-on.

8.0 Inquiries

Direct inquiries regarding this policy to:

OLLEISN help desk support (614) 644-8747.