**Section 1240.50 LEADS Access Security**

a) Each LEADS participating agency shall comply with the LEADS access security standards established by the Department.

b) Personnel Security Requirements

1) Thorough background screening of LEADS-related personnel is required by the employing agency. State and national criminal history record checks by fingerprint identification must be conducted for terminal operators, programmers, and other persons employed or utilized to effectuate access to or initiate transmission of LEADS and National Crime Information Center (NCIC) information, regardless of the frequency of access. A fingerprint-based background check must be performed on any person with direct access to LEADS. The agency shall submit both Illinois and FBI criminal justice applicant fingerprint inquiries to the Illinois State Police, Bureau of Identification.

2) No persons will be permitted LEADS access unless they are of good character and have not been convicted of a felony or a crime involving moral turpitude under the laws of this or any other jurisdiction. Any person may have their LEADS access denied if charged with a felony or crime of moral turpitude under the laws of this or any other jurisdiction.

3) No person may provide maintenance or technical services at or near LEADS equipment unless they are of good character and have not been convicted of a felony or a crime involving moral turpitude under the laws of this or any other jurisdiction. Any persons may have their authority to provide maintenance or technical services at or near LEADS equipment denied if charged with a felony or a crime involving moral turpitude under the laws of this or any other jurisdiction.

4) LEADS operators shall use the terminal only for those purposes for which they are authorized. The individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the data.

5) Each participating criminal justice agency must have appropriate written standards for discipline of LEADS and NCIC policy violators.

c) Site Management Requirements

Each LEADS agency must ensure that all LEADS computer devices are placed in a location under the direct control and supervision of authorized criminal justice personnel and are inaccessible to the public or persons not qualified to either operate, view, or possess LEADS and/or NCIC transmitted or received data. The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.