661—81.3(692) Criminal intelligence file security. The intelligence bureau of the department of public safety shall adopt administrative, technical, and physical safeguards, including audit trails, to ensure against unauthorized access and against intentional or unintentional damage to the LEIN information system. These safeguards shall include, but are not limited to, the following:

81.3(1) Records indicating who has been given the information, the reason for release of information, and the date of any dissemination shall be maintained until the information has been purged.

81.3(2) Criminal intelligence files shall be labeled to indicate security level and identities of submitting agencies and submitting individual.

81.3(3) Where appropriate, effective and technologically advanced computer software and hardware designs shall be implemented to prevent unauthorized access.

81.3(4) Any access to criminal intelligence files and computing facilities in which the files are stored shall be restricted to authorized personnel.

81.3(5) Criminal intelligence files shall be stored in such a manner that the files cannot be modified, destroyed, accessed, purged, or overlaid in any fashion by unauthorized personnel.

81.3(6) Computer systems on which criminal intelligence files are stored shall be programmed to detect, reject, and record any unauthorized attempt to access, modify, or destroy criminal intelligence files or to otherwise penetrate the security safeguards on such a system.

81.3(7) Access to any information required to gain authorized access to criminal intelligence files, including access codes and passwords, shall be restricted only to personnel authorized to access these files. The intelligence bureau shall ensure that criminal intelligence files remain confidential when specific agreements are entered into with individuals or organizations that provide computer or programming support to the agency.

81.3(8) Procedures shall be adopted to protect criminal intelligence files from unauthorized access, theft, sabotage, fire, flood, wind, and natural or other disasters.

81.3(9) Procedures shall be adopted which establish the right of the intelligence bureau to screen and, if appropriate, reject for employment any personnel who would, if hired, have access to criminal intelligence files.

81.3(10) Procedures shall be established which allow the removal or transfer, based on good cause, of any existing employees from positions in which they have access to criminal intelligence files.

81.3(11) Any compromise, or suspected compromise, of information that would allow unauthorized access into criminal intelligence files shall be reported without delay and, in any event, by the end of the next business day, to a supervisor within the intelligence bureau of the department of public safety.

81.3(12) Any compromise, or suspected compromise, of information contained in criminal intelligence files shall be reported without delay and, in any event, by the end of the next business day, to a supervisor within the intelligence bureau of the department of public safety.