

**RULES
OF
TENNESSEE BUREAU OF INVESTIGATION**

**CHAPTER 1395-1-1
TENNESSEE CRIME INFORMATION CENTER**

TABLE OF CONTENTS

1395-1-1-.01	Short Title	1395-1-1-.06	Tennessee Information Enforcement System (TIES)
1395-1-1-.02	Statement of Intent and Application	1395-1-1-.07	Automated Fingerprint Information System (AFIS)
1395-1-1-.03	Definitions	1395-1-1-.08	Certification of Records
1395-1-1-.04	Applicability of Federal and State Laws, Rules, Regulations and Guidelines	1395-1-1-.09	Repealed
1395-1-1-.05	Scope of Rules	1395-1-1-.10	Repealed

1395-1-1-.01 SHORT TITLE. These rules shall be known and may be cited as the Rules of the Tennessee Crime Information Center.

Authority: T.C.A. §§38-10-103 and 38-6-107. *Administrative History:* Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.02 STATEMENT OF INTENT AND APPLICATION.

- (1) Intent - It is the intent of the Legislature to accumulate in one place all of the vital information relating to crimes, criminals and criminal activities generated by the actions of all state and local law enforcement agencies performing duties in relation thereto, thereby establishing a criminal justice information system for substantive use by all participants and statistical analysis and use by the government and private sectors. It requires the Director of the Tennessee Bureau of Investigation to construct the crime data elements by specifying the content and form of reports and to establish the communications system for intrastate submission and sharing of the data, by agreements between the Tennessee Bureau of Investigation, Federal Bureau of Investigation and National Law Enforcement Telecommunications Systems.
- (2) Application - To make the system complete and effective, the Legislature requires the participation of all state, county and municipal and correctional agencies and courts. The participation is made uniform, efficient and effective by the promulgation and adoption of rules by the Director of the Tennessee Bureau of Investigation.
- (3) System Scope - As mandated, TBI will design, procure, operate, manage and control computer hardware and associated software to enable it to establish a system for the intrastate communication and exchange of all vital information, including statistical analysis thereof, relating to crime, criminals and criminal activity. It will, at a minimum:
 - (a) Provide a communications network with adequate computer hardware and software for use by law enforcement agencies;
 - (b) Provide certainty of identification of people with their criminal activity and records;
 - (c) Create a data base for the storage, management and distribution of the vital crime information for maximum interactive and relational use; and
 - (d) Comply with all state and federal laws relating to the privacy and security of the data.
- (4) Interaction of Data Programs - It is the intent of the Tennessee Bureau of Investigation that this reporting and operating system be fully compatible with the requirements of all similar Federal

(Rule 1395-1-1-.02, continued)

programs. The duties required of all state and local agencies which participate in the criminal justice system are specified and regulated by numerous statutes and laws relating to the various agencies. It is not the intent of the rules promulgated herein to create new duties or activities, or to change existing required duties, but rather to provide a more precise, uniform and effective manner in which the information generated and used by the various agencies in their operations may be reported, collected, managed and distributed timely and efficiently for maximum use and effectiveness by all agencies having need thereof while maintaining the integrity of actions and files of all participating agencies.

- (5) Control - It is the intent of the Tennessee Bureau of Investigation to ensure that this reporting system fully complies with all federal and state constitutional, statutory, and case law protecting and regulating the rights of privacy and other individual rights.

Authority: T.C.A. §§38-6-109 and 38-10-101 through 103. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.03 DEFINITIONS.

- (1) Administration of Criminal Justice - The performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused person or criminal offenders; criminal identification activities; and the collection, storage, and dissemination of criminal history records and crime data information.
- (2) AFIS - Automated Fingerprint Identification System that contains the complete Bureau fingerprint files, which provide the certainty of positive identification of every criminal history, and the associated hardware/software required to manage this data.
- (3) Bureau - Tennessee Bureau of Investigation (TBI).
- (4) CFR - Code of Federal Regulations
- (5) CHRI - Criminal History Record Information in computerized form.
- (6) CHR - Criminal History Record of a person who has been arrested and charged with having committed a criminal offense.
- (7) Criminal Justice Agency - Means (a) courts; or (b) a governmental agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocate a substantial part of its annual budget to the administration of criminal justice (more than 50%) or performs a legally authorized function which results in arrest of accused persons and/or institution of criminal charges. State and Federal Inspector General offices are included.
- (8) Criminal Justice Information - Information received, generated, collected, modified, or artificially created by criminal justice agencies that is needed for the performance of their legally authorized functions. This includes, but is not limited to, information on: wanted persons, stolen property, criminal histories, commencement and termination of prosecution, identification of criminal acts and conduct; and information compiled in the course of the investigation of crimes that are known or believed on "justifiable suspicion" or reasonable grounds to have occurred, or to be in the planning or conspiratorial process, including information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor criminal activity, and information artificially created from the analysis and combination of other data.
- (9) CJIS - Criminal Justice Information Services, maintained by the FBI.

(Rule 1395-1-1-.03, continued)

- (10) CTA - Control Terminal Agency maintained by the TBI and approved by the FBI/NCIC for the State of Tennessee for control of the TIES network.
- (11) Director - The Director of the TBI.
- (12) Full Access - A TIES agency which makes entries into NCIC and TCIC files.
- (13) LAN - Local Area Network.
- (14) Law Enforcement Agency - A governmental agency having statutory power of arrest whose primary function is that of detection, apprehension, and institution of prosecutions and which allocates more than fifty percent (50%) of its budget to the administration of criminal justice. Includes all police and sheriffs departments and offices.
- (15) NCIC - National Crime Information Center, operated by the FBI.
- (16) NIBRS - National Incident Based Reporting System.
- (17) NIST - National Institute of Standards and Technology.
- (18) NLETS - National Law Enforcement Telecommunications System is a nonprofit incorporated organization made up of representatives of law enforcement agencies from each of the fifty (50) states, District of Columbia, Puerto Rico, and several federal law enforcement agencies.
- (19) Non-Terminal Agency - An agency accessing the TIES by means of a Terminal Agency.
- (20) POST - Police Officer Standards and Training.
- (21) Query-Only Access - A TIES agency that is programmatically prohibited from making entries into the NCIC and TCIC files.
- (22) Satellite - A Terminal Agency accessing the TIES through another agency's computer.
- (23) SID - State Identification Number, a unique identification number assigned by the TBI to each person for whom a criminal history is established pursuant to a fingerprint identification, or a number assigned to any other person for whom a file is required to be maintained by TBI pursuant to law but is not based upon a fingerprint identification.
- (24) TCIC - Tennessee Crime Information Center, operated by the TBI and required by Chapter 10 of Title 38 of the Tennessee Code Annotated.
- (25) Terminal Agency - An agency accessing the TIES by means of a computer system or terminal.
- (26) TIBRS - Tennessee Incident Based Reporting System.
- (27) TICIC - Tennessee Internet Crime Information Center.
- (28) TIES - Tennessee Information Enforcement System is a hardware/software system dedicated to linking law enforcement agencies with one another and/or with databases and transmitting law enforcement information.
- (29) TRAP - Tennessee Repository for the Apprehension of Persons is an automated tracking mechanism to assist in the apprehension and subsequent prosecution of fugitives from justice.

(Rule 1395-1-1-.03, continued)

- (30) UCR - Uniform Crime Reporting, operated by the FBI.
- (31) WAN - Wide Area Network.

Authority: T.C.A. §§38-6-107, 38-6-109, 38-6-116, and 38-10-101 through 103. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.04 APPLICABILITY OF FEDERAL AND STATE LAWS, RULES, REGULATIONS AND GUIDELINES.

- (1) The operations of the Tennessee Crime Information Center and all of its component systems are subject to and controlled by the federal and state constitutions, all applicable federal and state law, all rules, regulations and guidelines promulgated by NCIC and NLETS, and these rules.
- (2) The system design and operation shall protect the integrity, confidentiality, and privacy of crime data and information in the transmission, storage and use modes.
- (3) The following minimum standards will be followed:
 - (a) Prevention of willful disclosure or delivery to persons not authorized by law to receive or handle the data; and
 - (b) Use of facilities, equipment or personnel which would directly expose the information to unauthorized persons or place the equipment and facilities within the control of unauthorized persons who could gain unauthorized access to the data.

Authority: T.C.A. §§ 38-6-102(e), 38-6-107, 38-10-101, 38-10-103, 38-10-107, and 38-10-10. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.05 SCOPE OF RULES.

- (1) These rules and regulations govern the generation, reporting (collecting), management, analysis and dissemination of vital information and statistics relating to crime, criminals, and criminal activity, including uniform crime reports, and the system of communication to accomplish this.
- (2) These rules and regulations govern the procedures for the official attestation, sealing, and certification of records when required or authorized by law.

Authority: T.C.A. §§38-6-101, 38-6-102(e), 38-6-107, and 38-10-103. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.06 TENNESSEE INFORMATION ENFORCEMENT SYSTEM (TIES).

- (1) All of the official rules, regulations and operating procedures of the FBI, NCIC and NLETS are hereby adopted and made applicable to the operation of TIES.
- (2) Compliance - All Agencies having access to TIES as terminal or satellite terminal agencies shall comply with all rules, regulations and guidelines of NCIC, NLETS and TCIC.
- (3) Access - Only statutorily authorized agencies will be permitted to connect computer devices to the TIES. Terminals of statutorily authorized agencies not meeting the definition of a criminal justice or

(Rule 1395-1-1-.06, continued)

law enforcement agency will be limited to the contribution and acquisition of the data authorized by statute for said agencies and prohibited from accessing NCIC and NLETS terminals and data bases, which would be in violation of laws and rules governing these agencies. All statutorily authorized agencies will meet the following criteria:

- (a) Equipment - All terminal equipment and software interfaced to TIES and constituting a part of TIES shall be compatible, as determined by TBI, with the TIES equipment and protocol.
- (b) Classification of Agencies - Agencies interfacing computer terminals to the TIES or receiving information from TCIC are divided into the following nine classes.
 1. Class One shall consist of governmental law enforcement agencies or criminal justice agencies which meet the criminal justice agency definition and which operate terminals on a continuous basis, twenty-four (24) hours a day, seven (7) days a week. These agencies have full access and are directly connected to TBI.
 2. Class Two shall consist of governmental law enforcement agencies or criminal justice agencies or criminal justice agencies which meet the criminal justice agency definition and which may or may not operate terminals on a continuous basis, twenty-four (24) hours a day, seven (7) days a week. These agencies have query-only access and are directly connected to TBI.
 3. Class Three shall consist of governmental law enforcement agencies or criminal justice agencies which meet the criminal justice agency definition and which operate terminals on a continuous basis, twenty-four (24) hours a day, seven (7) days a week. These agencies have full access and are connected as Satellite Agencies to TBI through another agency's computer system.
 4. Class Four shall consist of governmental law enforcement agencies or criminal justice agencies which meet the criminal justice agency definition and which may or may not operate terminals on a continuous basis, twenty-four (24) hours a day, seven (7) days a week. These agencies have query-only access and are connected as Satellite Agencies to TBI through another agency's computer system.
 5. Class Five consists of agencies that operate a large-scale computer system directly interfaced with the TBI. These agencies have been approved by TBI to have sufficient staff and resources to provide security, training, and related computer services to other network agencies.
 6. Class Six shall consist of consolidated and computer-assisted dispatch facilities, often referred to as 911 facilities. These may be governmental or non-governmental facilities that operate on a continuous basis, twenty-four (24) hours a day, seven (7) days a week.
 7. Class Seven shall consist of non-criminal justice agencies that perform criminal justice functions.
 8. Class Eight shall consist of non-criminal justice agencies accessing in-state records.
 9. Class Nine shall consist of NLETS ORI access.
- (4) User Agreements - All agencies accessing the TIES shall execute a User Agreement with the TBI. Any agency providing TIES access to a non-terminal agency shall execute the appropriate agreement with that agency. Any Class Three agency providing access to another agency shall execute a User Agreement, which will include all requirements set out in a TBI User Agreement and any additional

(Rule 1395-1-1-.06, continued)

provisions deemed necessary by that agency. All agreements between agencies shall be approved by TBI. Class Seven agencies shall execute the required security addendum as provided by the FBI.

- (5) Audit - All agencies shall submit to FBI and TBI audit to ensure compliance with all FBI, NCIC, NLETS and TCIC rules. No TBI employee who is responsible for auditing local law enforcement agencies shall conduct an audit of an agency by which the employee was employed in the past in any capacity. This applies regardless of the length of service and/or the time since service with the prior employer.
- (6) Access Cost - All directly connected terminal agencies will share in the costs incurred by TBI in the day-to-day operations of the TIES and associated communication network.
- (7) Any terminal agency, upon approval by TBI, is authorized at its own expense to furnish a terminal to another agency for operation as a satellite upon execution of an agreement requiring servicing of said terminals and operation thereof to meet minimum NCIC, NLETS and TCIC standards without degradation of TIES.
- (8) Any agency desiring to connect to the TIES shall make a request in writing to the TBI. Upon securing the approval of TBI, the agency shall execute and maintain an agreement. The agreement will require compliance with NCIC, NLETS, TCIC rules and regulations, operation to comply with all privacy laws, security of equipment, sharing of costs and performance of all things applicable to the appropriate class of agency required to make TIES an interactive system performing the duties and furnishing the benefits intended by Chapter 10 of Title 38 of T.C.A.
- (9) Absent provisions set forth in state law, Tennessee criminal history records are not accessible to the general public except under the following conditions:
 - (a) To challenge an arrest that appears on a criminal history record check conducted for employment, license or firearms carry permit or purchase.
 - (b) To challenge a criminal history record the individual must:
 1. submit a written request to the TBI Records and Identification Unit;
 2. provide satisfactory proof of identification including a photo ID;
 3. submit at least two (2) classifiable fingerprint cards for comparison; and
 4. pay a fee set by the Director as set forth in TCA 38-6-103(d)(1)(2).
- (10) Dissemination - Indirect dissemination of specific information received through the TIES shall be allowed unless there are specific state, local or federal laws precluding this dissemination. No agency authorized by statute to receive information from state CHRI shall use the information obtained there from for any purpose other than law enforcement purposes or as authorized by statute and is prohibited from disclosing, exposing or transmitting by any means information from TIES to any private citizen, corporation, entity or any other government agency not specifically authorized by statute to have such information.
- (11) Policy Violations - Any violations of policies governing the use and operation or information received from the TIES shall be reported immediately to the TBI.
- (12) Physical Security - Physical locations of all fixed agency terminals shall be approved by the TBI. The computer site and/or terminal area shall have adequate physical security to protect against any

(Rule 1395-1-1-.06, continued)

unauthorized personnel gaining access to the computer equipment or to any of the stored data. Prior approval shall be received from the TBI for additional devices to be connected to the TIES network.

- (13) System Security - All agencies shall demonstrate compliance with the current CJIS security policy published by the FBI. Class five agencies shall ensure and provide evidence to TBI that the system has ample hardware and software safeguards to limit TIES access to only authorized terminals and personnel of the satellite agency.
- (14) Qualifications -
- (a) Terminal operators who are public safety emergency dispatchers shall meet the qualifications in TCA § 7-86-201.
 - (b) Terminal operators who are not emergency dispatchers shall meet the following minimum qualifications.
 - 1. Be at least eighteen (18) years of age;
 - 2. Be a citizen of the United States;
 - 3. Be a high school graduate or possess equivalency;
 - 4. Have fingerprints on file with the TBI;
 - 5. Have no felony convictions; and
 - 6. Be of good moral character.
- (15) Certification - Certification requirements include, but are not limited to, the following:
- (a) All terminal operators must complete certification courses offered by TBI in order to operate the terminal equipment, or certification shall be issued upon successful completion of a training curriculum prescribed by the Information Systems division;
 - (b) All certified operators must be re-certified once every two (2) years by successfully completing all certification courses offered by TBI; and
 - (c) Only certified operators will be allowed to operate a TIES terminal (an exception being an operator-trainee who has not completed the initial certification program, in which case a certified operator must be present when the equipment is being operated by the trainee).
- (16) Training - Terminal agencies will require that their terminal operators attend training sessions offered by TBI to ensure proper operation of terminal equipment. Class five agencies shall provide TBI approved training for and certification of the Class five agency operators and satellite terminal agency operators.
- (17) Terminal Agency Coordinator - Each terminal agency shall appoint a Terminal Agency Coordinator to act as the liaison with TBI. The agency shall inform TBI of the Terminal Agency Coordinator assignment and any re-appointments that are made in said position. Re-appointments shall be made immediately upon the vacancy of a Coordinator's position. Any agency whose TAC or alternate TAC is convicted of a criminal offense while holding such position shall notify TBI of such conviction immediately.

(Rule 1395-1-1-.06, continued)

- (18) TIES - Terminal agencies are authorized to transmit, receive or exchange information directly relating to law enforcement, but shall not use the system for the transmission of general or personal messages. TIES terminal stations, which are used to make NCIC entries, shall be operated twenty-four (24) hours a day, seven (7) days a week. Terminal stations, both fixed and mobile, which are used for query-only, shall be secured when unattended.
- (19) Criminal History Inquiries - All criminal history inquiries and disseminations shall be logged with a hardcopy showing information received and the requesting person's authority for making the request. The log shall be maintained for two (2) years from the date of transmission.
- (20) Violations of Federal or State laws and NCIC, NLETS, and TCIC rules and regulations will result in the following disciplinary action:
 - (a) Willful violation of Federal law, T.C.A. § 39-3-Part 14 or § 40-32-101, will result in interruption of the interface of the terminal of the offending agency, and restoration will be made when the offending agency has furnished proof of appropriate action to correct the offense and assure future compliance;
 - (b) Willful violation of rules and regulations or other laws, including unauthorized access of files or unauthorized disclosure of data obtained for lawful purposes, will result in a required formal notification, within a specified time, of the violation with an explanation of the correction and conditions or circumstances which produced the violation(s);
 - (c) Any unauthorized acquisition and/or use of data relating to a specific person will require notification to the affected person by the offending agency or in lieu thereof, by TBI; and
 - (d) Continued violations of the same kind or frequent violations after warnings will result in cancellation of the user agreement and discontinuance of the TIES access to the agency.
- (20) Equipment software will contain provisions for classification of data. All data transmitted over TIES is classified as follows:
 - (a) Class A shall include any data the disclosure of which to unauthorized persons, or agencies or entities would constitute a violation of the criminal laws;
 - (b) Class B shall include any data which is rendered confidential by a specific law or court decision;
 - (c) Class C shall include data which the judiciary has determined to be private as protected by the United States Constitution and related laws;
 - (d) Class D shall include any data which may be restricted by court order incident to a judicial proceeding;
 - (e) Class E shall include all TBI case file information relating to specific crimes, criminal activity and persons;
 - (f) Class F shall include all other general data relating to crimes, criminals and criminal activities, which may be disclosed to the public.
- (21) All criminal history record information or any other information protected by a privacy law received from NCIC through TIES will carry a privacy classification designation contained within equipment software which will attach to all subsequent transmission of that data by any means. Also, if any data is received through the system by an agency, which is not classified but becomes classified because of

(Rule 1395-1-1-.06, continued)

any laws relating to that agency, then any subsequent dissemination of that information by that agency shall carry its privacy classification.

- (22) All agencies, which have been identified by NCIC and TCIC as being agencies authorized to handle data in relation to any of the programs and files maintained by NCIC and TCIC, shall be entitled to access the information in relation to those programs from both NCIC and TCIC files.

Authority: T.C.A. §§38-6-102(e), 38-6-103, and 38-10-101. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.07 AUTOMATED FINGERPRINT INFORMATION SYSTEM (AFIS).

- (1) Fingerprints of persons arrested and submitted under existing state law shall be subject to the following regulations of the AFIS System:
- (a) Fingerprints shall be retained in the AFIS database until the person reaches the age prescribed for removal of the record under RDA 1686;
 - (b) Fingerprints may be submitted by mail or by any electronic means meeting NIST standards as defined in the TBI Electronic Fingerprint Submission Interface Specifications;
 - (c) Fingerprints not meeting the TBI quality control standards shall be rejected and returned to the contributor with a standardized rejection form attached describing the reason(s) for rejection;
 - (d) Fingerprints of juveniles will be retained only if they meet quality control standards and contain one of the following notations:
 - 1. Treat as Adult; or
 - 2. Juvenile Felony Arrest.Arrest histories generated from juvenile fingerprint receipts meeting the above criteria will be disseminated in the same manner as adult records;
 - (e) TBI will report statistics related to fingerprint submissions and rejections to the State Comptroller's office; and
 - (f) Records will be removed only on the receipt of a court ordered expungement, death notice, or receipt of official request on departmental letterhead from the head of the submitting agency.
- (2) Law Enforcement and Criminal Justice Agency Applicant Fingerprints shall be subject to the following regulations:
- (a) Candidates for sheriff will submit two (2) sets of fingerprints on form FD-258. The cards should bear the TBI's ORI. The "Reason Fingerprinted" block of the form shall bear the notation "Candidate for sheriff of (name of) county;" and
 - (b) Any CHR located as a result of fingerprint search of law enforcement, criminal justice agency applicants or employees, and candidates for sheriff will be reported to the contributing agency, with a copy forwarded to the POST commission. Any CHR located on sheriff's candidates will be reported to the District Attorney General or other contributing agency.
- (3) Regulatory and Other Non-Criminal Justice Agencies shall be subject to the following regulations:

(Rule 1395-1-1-.07, continued)

- (a) Agencies which issue licenses or permits to any person, corporation, partnership, or other entity to engage in an authorized activity affecting the rights, property, or interests of the public or segments thereof, may submit fingerprints as required by enabling legislation for the limited purpose of determining if such license or permit should be issued; and
- (b) Processing fees will be assessed and collected by the TBI in accordance with existing state law. Fees will be collectible in advance by cashier's check, certified check, money order, or by journal voucher to state agencies.

Authority: T.C.A. §§38-6-102(e), 38-6-103, 38-10-101, and 37-10-207. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1-.08 CERTIFICATION OF RECORDS.

- (1) It is the purpose of these rules relating to certification to provide the certainty of the official authorization of records of the Bureau whenever official attestation, sealing, and certification of the TBI records, reports, documents, and actions are required by law, including orders of the courts, but not to create any greater or additional coverage of certification than authorized by law.
- (2) Every report of the Forensic Services Division rendered or administered in connection with any case in a criminal, juvenile, or municipal court, or when otherwise required by law, or dealing with alcohol or drug content of blood, breath or urine shall bear the following certification:

I certify and attest that this document is the proper record it purports to be.

/s/ _____
 Designated Representative of TBI Director

- (3) The following persons shall be responsible for the certification of any Forensic Services Division report prepared at a TBI facility under their supervision:
 - (a) TBI Assistant Director for Forensic Services; or
 - (b) Any Crime Laboratory Regional Supervisor.
- (4) The certification of criminal histories, when required by law, shall bear the certification in (2) above, and shall also contain the following certification:

I hereby attest that the above is a true and accurate xerographic representation of the fingerprints of: _____ as maintained by the State Central Repository of Criminal History Records by the Records and Identification Unit of the Tennessee Bureau of Investigation. I further attest that I am the Supervisor of the Records and Identification Unit and Official Custodian of Records for the Tennessee Bureau of Investigation.

 Signature of Custodian of Records

 Typed or Printed Name

 Date

(Rule 1395-1-1-.08, continued)

- (5) The attestation, scaling and certification of TBI records, reports, documents, and actions other than those listed above, including the authentication of identification of Bureau personnel with the public and internal documents of the Bureau, shall be executed by the Director or Deputy Director.
- (6) All certification shall contain the official Tennessee Bureau of Investigation Seal as follows:

When the seal is used, it may be affixed by being printed or impressed.



Authority: T.C.A. §§10-7-504, 37-10-102, 37-10-203, 37-10-205, 38-6-107, 38-6-109, 38-6-110, 38-10-101, 39-32-101, 39-32-104, 40-32-101, and 40-32-104. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repealed and new rule filed November 16, 2001; effective March 30, 2002.

1395-1-1.09 REPEALED.

Authority: T.C.A. §§37-10-207, 38-6-103, and 38-10-101. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Amendment filed October 25, 1988; effective January 29, 1989. Repeal filed November 16, 2001; effective March 30, 2002.

1395-1-1.10 REPEALED.

Authority: T.C.A. §38-6-107. **Administrative History:** Original rule filed October 30, 1986; effective January 27, 1987. Repeal filed November 16, 2001; effective March 30, 2002.