ARTICLE 5. COMMUNICATION SYSTEMS

Rule 1. Indiana Data and Communications System–Policy

240 IAC 5-1-1 General policy; restrictions on use

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 1. (a) A committee appointed by the superintendent of the Indiana state police, for the purpose of managing and controlling the Indiana data and communications system, hereinafter called "IDACS", has the responsibility for the management of the statewide system network as imposed by this article and as directed by the superintendent of state police. The committee chairman shall be selected by the superintendent. The chairman shall report activities of the committee to the superintendent for review and approval. To assure the proper operation of the system, the standards, procedures, formats, and criteria as set forth herein shall be strictly adhered to. In this respect, as in system security, the IDACS terminal agency shall not only follow the rules set forth, but shall also ensure that agencies they are servicing do the same.

(b) Accuracy is essential as is promptness in entering, modifying, locating, or clearing records in the system. Each record on file is identified with the agency originating that record, and that agency alone is responsible for the accuracy, completeness, and correct status of that record at all times. IDACS cannot assume responsibility for the accuracy of any records entered by any agency.

(c) The IDACS provides information for decision making, by investigators and patrolmen. The information furnished through IDACS shall be evaluated with other facts known to the officer and investigators at the scene. IDACS is an information tool. It is no substitute for professional police judgment.

(d) When an agency receives a positive response (wanted notice) from IDACS or NCIC, an immediate follow-up confirmation request with the agency that originated the record in the system is necessary before any enforcement action is taken. Likewise, the originating agency has an obligation to supply a substantive response within ten (10) minutes to the inquiring agency. This response shall include a confirmation or denial of the wanted notice or the length of time it will take to respond.

(e) IDACS is primarily a system for law enforcement/criminal justice users, and as such only data related to law enforcement/criminal justice shall be transacted by the system. Information furnished through the system shall be restricted to the use of authorized law enforcement/criminal justice agencies, or those authorized noncriminal justice agencies performing criminal justice responsibilities, and shall not be sold, transmitted, or disseminated to any noncriminal justice agency or person unless authorized by the state police superintendent. Such authorization for dissemination can occur when it has been determined that to do so would be in the best interest of the law enforcement/criminal justice community. *(State Police Department; Ch I, Prelim; filed Dec 20, 1978, 2:43 p.m.: 2 IR 136; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; errata, 6 IR 777; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2098; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

240 IAC 5-1-2 Audit of system transactions

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-5

Sec. 2. (a) Established IDACS committee policy requires all user agencies to maintain an audit trail for six (6) months for certain types of IDACS transactions as itemized but not limited to the following:

(1) Switched messages (both transmitted and received).

(2) Bureau of motor vehicles and department of natural resources information file data.

(3) IDACS/NCIC stolen file data.

(4) Out-of-state (NLETs) bureau of motor vehicles or department of natural resources data.

These audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. Audit trails shall be maintained manually or by automation, and shall be made available to the IDACS committee for inspection upon request.

(b) It should be noted that these are minimum requirements, and it may be necessary to keep important or case related traffic for longer periods of time in order to properly confirm or validate IDACS/NCIC wanted entries. *(State Police Department; Ch I, Retention of IDACS; filed Dec 20, 1978, 2:43 p.m.: 2 IR 137; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2098; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

240 IAC 5-1-3 Audit of criminal history record dissemination

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6; IC 10-13-2-5

Sec. 3. 28 U.S.C. states that audits shall be kept pertaining to the dissemination of criminal history records. This includes responses from NCIC's Interstate Identification Index (NCIC III) and responses from state central repositories and other agency criminal history files (both in-state and out-of-state). Such audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. *(State Police Department; Ch I, Criminal History Record Dissemination and Retention; filed Dec 20, 1978, 2:43 p.m.: 2 IR 137; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2099; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

Rule 2. Indiana Data and Communications System – Security

240 IAC 5-2-1 "System" defined *(Repealed)*

Sec. 1. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-2 Who may access criminal history data *(Repealed)*

Sec. 2. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-3 Control of criminal justice records systems *(Repealed)*

Sec. 3. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-4 Use of system-derived criminal history data *(Repealed)*

Sec. 4. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-5 Right to challenge record *(Repealed)*

Sec. 5. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-6 Physical, technical and personnel security measures *(Repealed)*

Sec. 6. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-7 Validation of records

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2

Sec. 7. (a) All IDACS user agencies shall validate, on a periodic basis, as prescribed to the user agency by IDACS, all IDACS wanted records entered on their authority. Validation of records shall be in conformity and compliance with rules set forth by IDACS.

(b) Validation obligates the originating agency to confirm the record is COMPLETE, ACCURATE, and is still OUTSTANDING or ACTIVE.

(c) Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the originating agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority shall make a determination based on the best information and knowledge available whether or not to retain the original entry on file.

(d) To ensure the validity of IDACS and NCIC records, administrative controls shall be maintained which will result in prompt updating for the benefit of system users. Agencies entering records in IDACS and/or NCIC are solely responsible for their accuracy, timeliness, and completeness. Only by conscientious validation of records can users remain assured the integrity of the system is being upheld, and inquiring officers can rely on the information in IDACS and NCIC.

(e) The Indiana control terminal (Indiana state police) is responsible to the national network (NCIC). Control terminal responsibilities are as follows:

(1) Monitor system use.

(2) Enforce discipline.

(3) Assure system procedures and policies are met by all users.

(f) Maintain validation schedule as established by NCIC/IDACS.

(g) Procedures for documentation are as follows:

(1) Each agency shall receive a validation printout in compliance with the validation schedule.

(2) It shall be the responsibility of the originating agency IDACS coordinator to cause each record to be processed according *[sic.]* subsection (c) and to ensure that any errors are corrected, inactive records are removed, and active records are kept in the system by submitting the appropriate validation transaction.

(h) Any record not appropriately validated within the authorized validation period shall be removed automatically from IDACS/NCIC.

(i) An agency that allows IDACS to purge inactive or unwanted records from the wanted files shall be subject to sanction. *(State Police Department; Ch I, Validation Policy; filed Dec 20, 1978, 2:43 p.m.: 2 IR 139; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2099; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

240 IAC 5-2-8 Terminal agency operation; coordinator; duties and responsibilities

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2-5

Sec. 8. Once operational on the IDACS system, each terminal agency is required to designate one (1) individual as coordinator to serve as liaison between that department and the IDACS committee. It is important that the person selected becomes familiar with all phases of IDACS to efficiently carry out all duties and responsibilities assigned. Duties and responsibilities are as follows:

(1) Ensure that all agency personnel (including any nonterminal agencies serviced) utilizing system information are aware of the rules and policies of the IDACS/NCIC/NLETS system.

(2) Disseminate the contents of the IDACS/NCIC newsletters to all terminal operators.

(3) Ensure that validation reports are properly processed.

(4) Ensure that terminal operators receive proper IDACS training in accordance with the IDACS certification training program.

(5) Maintain NCIC and IDACS manual revisions and disseminate information to operators.

(6) Advise IDACS of any changes in the agency head, the coordinator, agency address, or terminal site.

(7) Report all IDACS rule violations and other improper uses to IDACS.

(State Police Department; Ch I, Validation of Agency Operation–Internal; filed Dec 20, 1978, 2:43 p.m.: 2 IR 139; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2490; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2100; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)

240 IAC 5-2-9 User agreement

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2-6

Sec. 9. All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana state police and the IDACS committee. Nonterminal agencies shall complete an agreement with the terminal agency that services them. *(State Police Department; Ch I, Sample Agreement; filed Dec 20, 1978, 2:43 p.m.: 2 IR 140; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2490; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2100; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

240 IAC 5-2-10 Security; confidentiality

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2

Sec. 10. (a) "System", as used in the security and confidentiality rules, means IDACS, NLETS, and/or NCIC terminals, equipment, and any and all data accessible from or stored therein.

(b) Access, meaning the ability to obtain information from the system, shall be permitted only to criminal justice agencies in the discharge of their official mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Release of Indiana bureau of motor vehicles data to noncriminal justice agencies may occur when it is determined to be in the best interest of law enforcement/criminal justice to do so. Agencies that shall be permitted access to SYSTEM data include the following:

(1) Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.

(2) Prosecutive agencies and departments at all governmental levels.

(3) Courts at all governmental levels with a criminal or equivalent jurisdiction.

(4) Correction departments at all governmental levels, including corrective institutions and probation departments.

(5) Parole commissions and agencies at all governmental levels.

(6) Agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information.

(7) Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

(c) Approved noncriminal justice agencies may have access to SYSTEM data on a limited basis. "Limited basis" means

restricted to only that data recommended through resolution by the IDACS committee and approved by the state police superintendent.

(d) All computers, electronic switches, and manual terminals (including mobile data terminals/printers) interfaced with the SYSTEM computer for the exchange of SYSTEM data shall be under the management control of criminal justice agencies. Similarly, satellite computers and manual terminals accessing the SYSTEM shall be under the management control of a criminal justice agency.

(e) "Management control" means the authority to set and enforce:

(1) priorities;

(2) standards for the selection, supervision, and termination of personnel; and

(3) policy governing the operations of computers, circuits, and telecommunications terminals used to process SYSTEM information insofar as the equipment is used to process, store, or transmit SYSTEM information.

Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the computerized SYSTEM. Management control shall remain fully independent of noncriminal justice data systems, and criminal justice systems shall receive priority service and be primarily dedicated to the service of the criminal justice community.

(f) In those instances where criminal justice agencies are utilizing equipment and personnel of a noncriminal justice agency for SYSTEM purposes, they shall have complete management control of the hardware and the people who use and operate the system.

(g) The criminal justice agency shall exercise management control with regard to the operation of the equipment by:

(1) having a written agreement with the noncriminal justice agency operating the data center providing the criminal justice agency authority to select and supervise personnel;

(2) having the authority to set and enforce policy concerning computer operations; and

(3) having budgetary control with regard to personnel and equipment in the criminal justice agency.

(h) Procedures for the use of system-derived criminal history data shall be as follows:

(1) Criminal history data on an individual from the national computerized file shall be made available outside the federal government to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing (except when a federal, state, or local law/ordinance exists making the criminal justice agency responsible for the processing or issuing of the licenses/permits) applications, or local or state employment, other than with a criminal justice agency, or for other uses unless such dissemination is pursuant to state and federal statutes or state and federal executive order. There are no exceptions.

(2) Researchers using the data shall acknowledge a fundamental commitment to respect individual privacy interests by removing the identification of subjects as fully as possible from the data. Proposed programs shall be reviewed by the IDACS committee to assure their propriety and to determine that proper security is being provided. All noncriminal justice agency requests involving the identities of individuals in conjunction with their national criminal history records shall be approved by the NCIC advisory policy board through the IDACS committee. The NCIC or the IDACS committee shall retain rights to monitor any research project approved and to terminate same if violation of the above principles is detected. Research data shall be provided off line only.

(3) Upon verification that any agency has received criminal history information and has disclosed that information to an unauthorized source, immediate action shall be taken by the IDACS committee. Unauthorized use of criminal history information shall result in imposed sanctions as authorized by this article.

(4) Agencies are instructed that their rights to direct access to NCIC information encompass only requests reasonably connected with their criminal justice responsibilities.

(5) The IDACS committee shall make checks as necessary concerning inquiries made of the SYSTEM to detect possible misuse.

(i) The person's right to see and challenge the contents of his records shall form an integral part of the SYSTEM with reasonable administrative procedures. If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC III file, or the state central repository, it shall be available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Such requests shall be made by the person contacting the FBI or state central repository directly, and not through the SYSTEM.

(j) The following security measures are the minimum to be adopted by all agencies having access to the SYSTEM data and are designed to prevent unauthorized access to the SYSTEM data and/or unauthorized use of that data:

(1) Security measures for computer centers as follows:

(A) All computer sites accessing SYSTEM data shall have the security to protect against any unauthorized access to any of the stored data and/or the computer equipment including the following:

(i) All doors having access to the central processing unit (CPU) room shall be locked at all times.

(ii) A visitor's log shall be maintained of all persons entering the CPU area except those assigned to the area on a permanent basis. The visitor's name, date, time in, time out, agency represented, and reason for visit.

(B) Since personnel at these computer centers have access to data stored in the SYSTEM, they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative. This screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigation, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as to the applicant's honesty, integrity, and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Also, convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the state police superintendent for a final approval or disapproval decision.

(C) All visitors to these computer centers shall be accompanied by a permanent full-time employee of the data center.

(D) Computers having access to the SYSTEM shall have the proper computer instructions written and other built-in controls to prevent SYSTEM data from being accessible to any terminals other than authorized terminals. These instructions and controls shall be made available to the IDACS committee for inspection upon request.

(E) Computers and/or terminals (including mobile data terminals) having access to SYSTEM data shall maintain an audit of all transactions. This audit trail shall be maintained either manually by each agency or automated by the computer center. This transaction audit shall be monitored and reviewed on a regular basis to detect any possible misuse of SYSTEM data. This audit shall be made available to IDACS for inspection upon request.

(2) Security measures for communications as follows:

(A) Lines/channels being used to transmit SYSTEM information shall be dedicated solely to SYSTEM use, i.e., there shall be no terminals belonging to agencies outside the criminal justice system sharing these lines/channels except by prior IDACS committee approval.

(B) Security of the lines/channels shall be established to protect against clandestine devices being utilized to intercept or inject SYSTEM traffic.

(C) Audio response terminals, radio devices, and mobile data terminals, whether digital (teleprinters) or voice, shall not be used for the transmission of criminal history data beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. Transmission shall be made to police officers upon his or her request.

(3) Security measures for terminal devices having access to the SYSTEM as follows:

(A) All agencies and computer centers having terminals on the SYSTEM and/or having access to SYSTEM data shall physically place these terminals in a secure location previously approved by the IDACS committee within the authorized agency. Subsequent physical location changes of terminals shall have prior approval of the IDACS committee.

(B) The agencies having terminals with access to SYSTEM data shall have terminal operators screened as in subdivision (1)(B) and restrict access to the terminal to a minimum number of authorized employees.

(C) Copies of SYSTEM data obtained from terminal devices shall be afforded security to prevent any unauthorized access to or use of that data. Copies of SYSTEM data which are no longer relevant shall be destroyed.

(D) Mobile teleprinters having access to SYSTEM data shall afford security to that data in the same manner as a fixed terminal. Any positive "wanted response" shall be duplicated at the agencies station terminal for proper interpretation and confirmation to occur. SYSTEM data shall not be transmitted to the device when it is unattended.

(State Police Department; 240 IAC 5-2-10; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2492; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2102; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)

240 IAC 5-2-11 IDACS operator/coordinator certification training

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 11. (a) All IDACS terminal operators (including mobile terminals) shall be trained and tested for their proficiency at operating the IDACS terminal. All IDACS coordinators shall be trained and tested for their proficiency at operating the IDACS terminal and for their skills as the coordinator.

(b) The objectives of training requirements shall be as follows:

(1) To ensure that terminal operators and coordinators are familiar with the laws governing IDACS/NCIC/NLETS, IDACS system rules, regulations, and procedures, and what files (functions) are available and how to utilize them properly.

(2) Create an awareness of IDACS/NCIC/NLETS system capabilities in order to allow criminal justice agencies to obtain maximum use of the system.

(c) All persons assigned a system password (operator identifier) to operate the IDACS terminal and persons designated IDACS coordinator by their agency shall be trained and tested according to the guidelines set forth by the IDACS committee and approved by the state police superintendent.

(d) Training course content shall be derived from the IDACS/NCIC/NLETS manuals and publications and be periodically reviewed for relevancy and accuracy and updated accordingly.

(e) The IDACS committee can authorize the removal of a system password or impose sanctions on an agency for noncompliance with these procedures. *(State Police Department; 240 IAC 5-2-11; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2105; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)*

240 IAC 5-2-12 User agency sanctions

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 12. (a) The IDACS committee shall review violations of IDACS rules and make recommendations to the state police superintendent to impose sanctions on user agencies.

(b) The objectives of the sanction procedure shall be as follows:

(1) To ensure the integrity of the SYSTEM.

(2) Create an awareness among user agencies of the importance of following rules, regulations, and procedures in order to minimize the risk to liabilities that may be incurred by misuse of the SYSTEM and its data.

(c) Sanctions shall be based upon the class of violation, any previous violations, and any exposure to criminal and civil liabilities that the violation might place on the SYSTEM, its officials, and the offending agency.

(d) Violations shall be classed as either administrative (minor) or security (serious) violations. Security violations being defined as one which has or could result in access of SYSTEM data by unauthorized individuals. All other violations are classed as administrative.

(e) In determining the severity of the violation, the violation type, either administrative or security, and previous sanctions issued, if any, shall be considered. The IDACS committee may impose as sanctions one (1) of the following:

(1) Verbal warning.

(2) Written warning.

(3) Written notice of violation.

(4) Written notice of probation.

(5) Written notice of temporary suspension.

(6) Written notice of permanent suspension.

(f) Temporary or permanent suspension of service will not begin, unless an emergency exists, until fifteen (15) days after the agency head has received written notice by certified mail or personal service.

(g) An agency may after one (1) year apply to be reinstated if placed on permanent suspension. *(State Police Department; 240 IAC 5-2-12; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2105; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2,*

2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA; readopted filed Nov 30, 2020, 2:49 p.m.: 20201230-IR-240200497RFA)

Rule 3. Indiana Law Enforcement Emergency Network–Administration *(Expired)*

(Expired under IC 4-22-2.5, effective January 1, 2014.)

Rule 4. Indiana Law Enforcement Emergency Network–Operational Procedures *(Expired)*

(Expired under IC 4-22-2.5, effective January 1, 2014.)

Rule 5. Indiana Law Enforcement Emergency Network–System Violation Reports *(Expired)*

(Expired under IC 4-22-2.5, effective January 1, 2014.)

*