

Table of Contents

11.10.01 - RULES GOVERNING ILETS - IDAHO LAW ENFORCEMENT TELETYPEWRITER SYSTEM

000. LEGAL AUTHORITY.....	2
001. TITLE AND SCOPE.....	2
002. WRITTEN INTERPRETATIONS.....	2
003. ADMINISTRATIVE APPEALS.....	2
004. INCORPORATION BY REFERENCE.....	2
005. MAILING ADDRESS AND OFFICE HOURS.....	2
006. -- 009. (RESERVED).....	2
010. DEFINITIONS.....	2
011. (RESERVED).....	4
012. EXECUTIVE OFFICER OF THE BOARD.....	4
013. ILETS BOARD; MEETINGS AND QUORUM.....	4
014. ILETS BOARD; POWERS AND DUTIES, CHAIRMAN, AND AD HOC ADVISORY COMMITTEES.....	5
015. ILETS BOARD; RESIGNATIONS AND REPLACEMENTS, NOTIFICATION.....	5
016. ILETS NETWORK.....	5
017. AGENCY ACCESS TO ILETS.....	6
018. USER ACCESS FEES.....	6
019. ADJUSTED ACCESS FEES DURING PILOT PROJECTS.....	8
020. USER RESPONSIBILITIES.....	8
021. INFORMATION ACCESS AND DISSEMINATION.....	8
022. -- 023. (RESERVED).....	9
024. ILETS SECURITY.....	9
025. -- 027. (RESERVED).....	11
028. USER AGENCY SANCTIONS.....	11
029. -- 999. (RESERVED).....	12

**IDAPA 11
TITLE 10
CHAPTER 01**

**11.10.01 - RULES GOVERNING ILETS - IDAHO LAW
ENFORCEMENT TELETYPEWRITER SYSTEM**

000. LEGAL AUTHORITY.

Title 19, Chapter 52, Idaho Code, creates a teletypewriter communications board and authorizes it to make rules necessary to establish and operate the Idaho law enforcement teletypewriter system. (3-30-01)

001. TITLE AND SCOPE.

01. Title. These rules shall be cited as IDAPA 11.10.01, "Rules Governing ILETS - Idaho Law Enforcement Teletypewriter System". (3-30-01)

02. Scope. The rules relate to the governance and operation of the Idaho Law Enforcement Teletypewriter System. (3-30-01)

002. WRITTEN INTERPRETATIONS.

There are no written interpretations of these rules. (3-30-01)

003. ADMINISTRATIVE APPEALS.

Administrative appeals under this chapter shall be governed by the rules of administrative procedure of the attorney general, IDAPA 04.11.01, "Idaho Rules of Administrative Procedure of the Attorney General". (3-30-01)

004. INCORPORATION BY REFERENCE.

01. Incorporated Documents. IDAPA 11.10.01 incorporates by reference the full text of the requirement found in the following documents: (3-30-01)

a. "Criminal Justice Information Systems," 28 CFR Part 20 (1999); (3-30-01)

b. "Criminal Justice Information Systems--CJIS Security Policy," Federal Bureau of Investigation, National Crime Information Center (May 1999); (3-30-01)

c. "National Crime Information Center, Operating Manual," Federal Bureau of Investigation, National Crime Information Center (April 1, 1998) (3-30-01)

d. "National Law Enforcement Telecommunication System, Users Guide," NLETS, Users Guide, (November 7, 1997) (3-30-01)

e. "National Law Enforcement Telecommunication System, Policies and Procedures," NLETS, Policies and Procedures, (May 22, 1989) (3-30-01)

02. Document Availability. The above listed documents are available during normal working hours for inspection and copying at the Idaho State Police, Bureau of Criminal Identification, 700 South Stratford Drive, Meridian, Idaho. (3-30-01)

005. MAILING ADDRESS AND OFFICE HOURS.

The mailing address is Idaho State Police, Bureau of Criminal Identification, P.O. Box 700, Meridian, ID 83680-0700. The office hours are Monday through Friday, 8:00 a.m. to 5:00 p.m. (3-30-01)

006. -- 009. (RESERVED).

010. DEFINITIONS.

01. Administration Of Criminal Justice. (3-30-01)

- a.** Administration of Criminal Justice means performance of any of the following activities: (3-30-01)
 - i. Detection; (3-30-01)
 - ii. Apprehension; (3-30-01)
 - iii. Detention; (3-30-01)
 - iv. Pretrial release; (3-30-01)
 - v. Post-trial release; (3-30-01)
 - vi. Prosecution; (3-30-01)
 - vii. Adjudication; (3-30-01)
 - viii. Correctional supervision; or (3-30-01)
 - ix. Rehabilitation of accused persons or criminal offenders. (3-30-01)
- b.** The administration of criminal justice includes: (3-30-01)
 - i. Criminal identification activities; and (3-30-01)
 - ii. The collection, storage, and dissemination of criminal history record information. (3-30-01)
- 02. Associated System.** Any automated or manual information system that is accessible through ILETS. (3-30-01)
- 03. Criminal Justice Agency.** (3-30-01)
 - a.** Federal and state courts having jurisdiction to hear criminal matters; and (3-30-01)
 - b.** A government agency or a subunit of an agency that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of justice. (3-30-01)
- 04. Board.** The board created, pursuant to Title 19, Chapter 52, Idaho Code, to establish priorities and operational policies and procedures relating to ILETS. (3-30-01)
- 05. Department.** The Idaho Department of Law Enforcement, or successor agency. (3-30-01)
- 06. Executive Officer.** As provided by Title 19, Chapter 52, Idaho Code, means the director of the Idaho Department of Law Enforcement, or successor agency. (3-30-01)
- 07. III.** The Interstate Identification Index, which is a cooperative federal-state system for the exchange of automated criminal history records and, to the extent of their participation in the III system, the criminal history repositories of the states. (3-30-01)
- 08. ILETS.** The Idaho Law Enforcement Teletypewriter (telecommunication) system established by the director of law enforcement pursuant to Title 19, Chapter 52, Idaho Code, and includes all hardware, software, electronic switches, peripheral gear, microwave links, circuitry, and terminal devices that comprise the system and includes access to the system. (3-30-01)
- 09. Management Control Agreement.** A written agreement between a criminal justice agency and a non-criminal justice agency that provides services (dispatching, record keeping, computer services, etc.) to the

criminal justice agency. The agreement shall give the criminal justice agency authority to set and enforce policies governing the non-criminal justice agency's access to ILETS. (3-30-01)

10. NCIC. The Federal Bureau of Investigation, National Crime Information Center, which is a computerized information system that includes telecommunications lines and any message facilities authorized by law regulation, or policy approved by the United States Attorney General to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The system includes information in the III system. (3-30-01)

11. NLETS. The National Law Enforcement Telecommunication System, Incorporated, a national computerized message switching system that links national and state criminal justice information systems. (3-30-01)

12. Non-Criminal Justice Agency. A state agency, federal agency, or unit of local government that is not a criminal justice agency. The term does not refer to private individuals, corporations, or non-governmental agencies or organizations. (3-30-01)

011. (RESERVED).

012. EXECUTIVE OFFICER OF THE BOARD.

01. Authority Of Office. The executive officer shall represent the board in the day-to-day administration of ILETS and is responsible for ensuring that all policies and decisions of the board are promulgated pursuant to the authority of Chapter 52, Title 19, Idaho Code. The executive officer may delegate duties to employees and officers of the department and shall execute instruments for, and on behalf of, the board and ILETS. (3-30-01)

02. Additional Responsibilities. In addition to the responsibilities assigned to the office by statute, the executive officer is responsible for ensuring, subject to adequate legislative appropriations, that the board receives adequate staff support and that the following staff duties are performed: (3-30-01)

a. Preparation and dissemination of agendas, posting of legal notices of all meetings, and maintenance of a written record of the proceedings of board meetings; and (3-30-01)

b. Management and safekeeping of all documents relating to the board and ILETS operations. (3-30-01)

03. Governing Policies And Rules. The executive officer and any department employees and officials assigned by the executive officer to support ILETS operations will be governed by policies and rules of the State of Idaho and the department concerning, but not limited to, fiscal, purchasing, and personnel matters. (3-30-01)

013. ILETS BOARD; MEETINGS AND QUORUM.

01. Schedule Of Meetings. The board shall hold regular meetings at least twice annually and may hold special meetings at other times as the executive officer deems necessary or upon the written request of a majority of the board. The regular semi-annual meetings of the board shall be scheduled on such dates and at such times as the executive officer may determine after consultation with the members. Meeting announcements and agendas shall be mailed to each member not less than ten (10) working days before a regular meeting. (3-30-01)

02. Quorum. When meeting, four (4) members of the board shall constitute a quorum necessary for transacting business. (3-30-01)

03. Representation At Meetings. A board member may not appoint an alternate to attend a meeting and exercise the voting privilege of that member. (3-30-01)

04. Posting And Minutes Of Meetings. Board meetings shall be posted and conducted in compliance with the "Idaho Open Meeting Law", Sections 67-2340 through 67-2347, Idaho Code. Minutes of all regular and special meetings of the board shall be prepared and maintained by staff assigned by the executive director to support the board. (3-30-01)

014. ILETS BOARD; POWERS AND DUTIES, CHAIRMAN, AND AD HOC ADVISORY COMMITTEES.

01. Powers And Duties. Pursuant to its authority under Title 19, Chapter 52, Idaho Code, the board establishes policies relating to management and operation of ILETS. The board shall enforce compliance with all laws and regulations governing ILETS operations. (3-30-01)

02. Election Of Chairman. At the first regular meeting of a calendar year, the board shall elect from its membership a chairman by majority vote of the board. The chairman shall serve a term of one (1) year and may succeed himself. (3-30-01)

03. Presiding Officer. The chairman shall preside at all meetings and conduct the meetings pursuant to "Roberts' Rules of Order, Current Revised Edition". If the chairman is absent at a meeting, the executive officer shall preside at that meeting. (3-30-01)

04. Advisory Committees. With the approval of the board, the chairman may appoint ad hoc advisory committees to assist the board in the execution of its statutory duties. A committee may include non-board members who would be of value to the committee's assigned task. A committee shall include not less than one (1) member of the board. Committee reports shall be submitted to the board in writing. (3-30-01)

015. ILETS BOARD; RESIGNATIONS AND REPLACEMENTS, NOTIFICATION.

01. Members Who No Longer Qualify. Any board member who ceases to qualify as a member shall at once notify the Governor and the executive officer. (3-30-01)

02. Resignations. Any board member who desires to terminate that member's service on the board shall at once notify the Governor and the executive officer of that intention. (3-30-01)

03. Notification Of Relevant Professional Associations. The executive officer shall forward any notification received from a member to the relevant professional association representing Idaho sheriffs and chiefs of police. (3-30-01)

016. ILETS NETWORK.

01. Establishment. Pursuant to Title 19, Chapter 52, Idaho Code, the executive officer shall establish ILETS as a program of the department of law enforcement or successor agency. (3-30-01)

02. Responsibilities. The program established by the executive officer shall have the following responsibilities: (3-30-01)

a. Develop and operate a computerized criminal justice telecommunications and information system that provides message switching and record inquiry and retrieval capabilities. (3-30-01)

b. Publish an ILETS Operations Manual and distribute copies to each user agency. (3-30-01)

c. Function as the NCIC control terminal agency and the NLETS control terminal agency for the State of Idaho. (3-30-01)

d. Assist and train criminal justice agencies regarding information retrieved from ILETS and associated systems for use in administration of criminal justice. (3-30-01)

e. Develop and maintain linkages with the Idaho Transportation Department, Idaho Department of Correction, other agencies and systems to make appropriate information available to Idaho criminal justice agencies that will assist them in the enforcement of state criminal and traffic laws and regulations. (3-30-01)

f. Provide staff support to the ILETS board. (3-30-01)

g. Operate a program of record validation, quality control, and audits to ensure that records entered into ILETS and NCIC files by the department and user agencies are kept accurate and complete and that compliance with state and national standards is maintained. (3-30-01)

h. Create model management control agreements between criminal justice agencies and non-criminal justice agencies. (3-30-01)

i. Provide assistance and information access to non-criminal justice user agencies for statutory licensing, employment and regulatory purposes and for other purposes authorized by law and approved by the board. (3-30-01)

017. AGENCY ACCESS TO ILETS.

01. Authorized Agencies. Consistent with Title 19, Chapter 52, Idaho Code, which mandates the exclusive use of ILETS for law enforcement and traffic safety purposes, access to ILETS shall be restricted to the following governmental agencies: (3-30-01)

a. Criminal justice agencies; (3-30-01)

b. Non-criminal agencies that provide computer services, dispatching support, or other direct support service to one (1) or more criminal justice agencies, and which have signed an ILETS-approved management control agreement with the criminal justice agency; (3-30-01)

c. Non-criminal justice agencies with a statutory requirement to use information capabilities that may be available via ILETS, and use of terminal access will not adversely affect criminal justice agency users, and use of the terminal will be for the administration of criminal justice; and (3-30-01)

d. Non-criminal justice agencies that provide information or capabilities needed by criminal justice agencies for a criminal justice purpose, and access or use of a terminal will improve the ability to provide such information or capabilities. (3-30-01)

02. Management Control Agreements. The management control agreement between a criminal justice agency and a non-criminal justice agency will grant to the criminal justice agency the authority to set and enforce: (3-30-01)

a. Priorities of service; (3-30-01)

b. Standards for the selection, supervision, and termination of personnel authorized to access ILETS; and (3-30-01)

c. Policies governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit information to or receive information from ILETS. (3-30-01)

03. Board Approval. The board shall review all requests for access to ILETS and determine whether an agency meets the criteria for access and whether access is appropriate based on system resources. Approved non-criminal justice agencies may have access to ILETS information on a limited basis (for example, motor vehicle information only) as authorized by the board. (3-30-01)

018. USER ACCESS FEES.

01. Payment Of Fees Required. Any agency that has signed a user agreement with ILETS to have direct terminal or system access to the network must pay access and usage fees as provided in Section 018. (3-13-02)

02. ILETS Network User Access Fees. The access fees approved by the board and to be collected quarterly in advance by the department are as follows: (3-13-02)

a. An agency at the county or municipal level shall pay an annual fee of four thousand dollars (\$4,000) for each telecommunication line drop to the agency. (3-13-02)

b. An agency at the state, federal, or tribal level shall pay an annual fee of seven thousand dollars (\$7,000) for each telecommunication line drop to the agency. (3-13-02)

03. Usage Fee. Any agency that has signed a user agreement with ILETS to have direct terminal or system access to the ILETS network must pay quarterly a usage fee based on that agency's percentage of total annual messages sent and received by user agencies through the ILETS message switcher. The total percentage for an agency shall include the message traffic generated by any other agency authorized to access ILETS through that agency's direct terminal or system access. (3-13-02)

a. The usage fee shall be paid according to the following schedule:

Percentage of Total ILETS Message Traffic	Annual Usage Fee
0 - .25 %	\$500
.26 - .50 %	\$1,000
.51 - .75 %	\$2,000
.76 - 1.0 %	\$4,000
1.01 - 1.50 %	\$6,000
1.51 - 2.0 %	\$9,000
2.01 - 5.0 %	\$13,500
> 5.01 %	\$20,250

(3-13-02)

b. The department shall conduct an audit of ILETS message switcher traffic for even-numbered years to determine an agency's annual usage fee, which will be effective for two (2) years with the quarterly statement for the fee period beginning October 1 of odd-numbered years. (3-13-02)

c. If an agency discontinues direct terminal or system access to ILETS and acquires authorized access through another agency, the usage fee for the agency maintaining direct access shall be adjusted to reflect the combined historical usage. (3-13-02)

d. A new agency approved for direct ILETS access that does not have historical usage shall be assessed by the department an interim usage fee pending the next audit of ILETS message traffic. The department shall set an interim fee based on the agency's similarities to existing agencies with direct terminal or system access. An agency may appeal to the board the interim usage fee set by the department. (3-13-02)

e. As operator of ILETS, the department, in lieu of payment of fees, shall provide direct and in-kind support of network operations. The board shall review biennially the proportion of that support to the overall operating cost of the system. (3-13-02)

04. Billing And Payment. The department shall mail billing statements quarterly to all agencies with direct terminal or system access to ILETS. Payment of the fees is due by the first day of the month of each quarter (October 1, January 1, April 1, and July 1), unless it is a Saturday, a Sunday, or a legal holiday, in which event the payment is due on the first successive business day. (3-13-02)

05. Sanctions For Delinquency. Any user agency delinquent in payment of assessed fees shall be

subject to sanctions under Section 028.

(3-13-02)

019. ADJUSTED ACCESS FEES DURING PILOT PROJECTS.

The board may adjust access fees of user agencies participating in pilot projects being conducted by the department in behalf of ILETS. The fee adjustment shall be based on any cost savings, actual or anticipated, realized by the ILETS network.

(3-30-01)

020. USER RESPONSIBILITIES.

01. User Agreement. Any agency using a terminal to access ILETS, whether directly or through another agency, is responsible for adhering to all applicable ILETS rules and policies and must have signed an agreement with ILETS to that effect.

(3-30-01)

02. Record Validation. Any agency that enters information into ILETS or NCIC files is responsible for the accuracy, timeliness and completeness of that information. ILETS will send a record validation review list, regularly, to each agency. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the wanted person, missing person, and vehicle files. In the event the agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during an ILETS or NCIC audit. When the agency has completed the validation they must return a signed certification of their validity within an appropriate time as established by ILETS.

(3-30-01)

03. Minimum Training. Each agency employee who operates a terminal or computer to access ILETS must complete ILETS training at a level consistent with the employee's duties. Each employee who operates a terminal or computer to access ILETS must be re-certified by the agency every two (2) years per schedules and procedures as prescribed by ILETS.

(3-30-01)

04. Hit Confirmation. When another agency receives a positive record response (Hit) from ILETS or NCIC and requests confirmation of the status of the record (warrant, stolen vehicle, etc.), the agency responsible for entry of the record must respond within ten (10) minutes for urgent hit confirmation requests or within one (1) hour for routine hit confirmation requests, with an answer indicating the status of the record or indicating a time frame when the record status will be confirmed.

(3-30-01)

05. Terminal Agency Coordinators. The agency administrator of each agency with terminal or computer access to ILETS must designate one (1) or more terminal agency coordinators who shall be the primary contacts for all matters relating to use of ILETS by the agency. A terminal agency coordinator must complete ILETS training at the highest level required by any person in the agency.

(3-30-01)

06. Background Checks Of Terminal Operators Required. Policies for access to the FBI-NCIC system require background screening of all terminal operators with access to the NCIC system. For efficiency and consistency, the key elements of the NCIC background screening policies are also adopted for all ILETS access.

(3-30-01)

021. INFORMATION ACCESS AND DISSEMINATION.

01. General Policy. Information is made available to ILETS users from various sources and agencies, including ILETS and other state justice information system files, motor vehicle departments, NCIC, and NLETS. Each user must observe any restrictions placed on the use or dissemination of information by its source. It is ILETS' responsibility to advise user agencies of any restrictions which apply to any information accessed via ILETS.

(3-30-01)

02. Criminal History Records. Criminal history information on an individual accessed via ILETS from a state or national computerized file shall be made available only to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such information for use in connection with licensing applications; regulatory activities; or local or state employment, other than with a criminal justice agency.

(3-30-01)

03. Administrative Messages. An administrative message (AM) is a free text message from one (1) agency to one (1) or more agencies. All administrative messages transmitted via ILETS must be by the authority of an authorized user and must relate to criminal justice purposes or matters of interest to the user community. Administrative messages sent within Idaho, either statewide, regionally or to individual terminal identifiers are subject to the following restrictions: (3-30-01)

a. No messages supportive or in opposition to political issues, labor management issues, or announcements of meetings relative to such issues. (3-30-01)

b. No messages supportive or in opposition of legislative bills. (3-30-01)

c. No requests for criminal history record information. (3-30-01)

022. -- 023. (RESERVED).

024. ILETS SECURITY.

01. General Policy. The data stored in the ILETS, NCIC, and other criminal justice information system files is documented criminal justice information. This information must be protected to ensure its integrity and its correct, legal and efficient storage, dissemination and use. It is incumbent upon an agency operating an ILETS terminal, or a terminal on another system that has access to the ILETS network, to implement the procedures necessary to make the terminal secure from any unauthorized use and to ensure ILETS is not subject to a malicious disruption of service. ILETS user agencies shall participate in ILETS training and compliance activities to ensure that all agency personnel authorized to access the ILETS network are instructed in the proper use and dissemination of the information and that appropriate agency personnel are aware of security requirements and of the dangers to network integrity. ILETS retains the authority to disconnect a user agency or network connection when serious security threats and vulnerabilities are detected. (3-30-01)

02. Definitions. The following is a list of terms and their meanings as used in the ILETS security rule: (3-30-01)

a. Computer interface capabilities means any communication to ILETS allowing an agency to participate in the system using devices other than ILETS-provided terminal equipment. (3-30-01)

b. Firewall means a collection of components placed between two (2) networks that keep the host network secure by having the following properties: (3-30-01)

i. All traffic from inside the network to outside, and vice-versa, must pass through it; (3-30-01)

ii. Only authorized traffic is allowed to pass; and (3-30-01)

iii. The components as a whole must be immune to unauthorized penetration and disablement. (3-30-01)

c. ILETS security officer means the department staff member designated by the executive officer to monitor and enforce agency compliance with site and network security requirements. (3-30-01)

d. Peer networks means computer interfaces between cooperative governmental agencies in Idaho where none of the participating entities exercise administrative or management control over any other participating entity. (3-30-01)

e. Primary site means an agency that has management control of a computer system directly connected to ILETS. (3-30-01)

f. Untrusted system means a system that does not employ sufficient hardware or software integrity measures to allow its use for simultaneously processing a range of sensitive or confidential information. (3-30-01)

03. Site Security Agreements. To ensure agencies having computer interface capabilities to ILETS are fully aware of their duties and of the consequences of failure to carry out those duties, a written and binding security agreement shall exist between ILETS and all primary sites. This agreement will clarify that the primary site is equally responsible for actions by secondary and affiliated systems connected through their site to ILETS. Primary sites must put in place similar subsidiary security agreements with secondary and affiliated systems to protect its network and ILETS. A site security agreement shall be an addendum to the ILETS user agreement. (3-30-01)

04. ILETS Security Officer. The ILETS Security Officer shall be responsible for the following duties: (3-30-01)

- a.** Disseminating to user agencies copies of ILETS security policies and guidelines; (3-30-01)
- b.** Communicating to user agencies information regarding current perceived security threats and providing recommended measures to address the threats; (3-30-01)
- c.** Monitoring use of the ILETS network either in response to information about a specific threat, or generally because of a perceived situation; (3-30-01)
- d.** Directing a primary site, through its nominated contact, to rectify any omission in its duty of responsibility; (3-30-01)
- e.** When an agency is unable or unwilling to co-operate, reporting the issue to the executive officer and initiating the procedure for achieving an emergency disconnection; and (3-30-01)
- f.** Provide support and coordination for investigations into breaches of security. (3-30-01)

05. Agency Security Contacts. A terminal agency coordinator shall serve as that agency's security contact for ILETS, unless another individual is specifically selected for this purpose and approved by the ILETS Security Officer. ILETS primary sites shall ensure the agency's security contact, or another person or position designated in an incident contingency plan, can be contacted by the ILETS security officer at any time. (3-30-01)

06. Peer Networks. The security responsibilities of the operators of peer networks connected to ILETS, with respect to their user organizations, are parallel to those of ILETS user organizations in respect to their individual users. The ILETS Security Officer shall ensure that a written agreement exists between ILETS and a primary site, signed by the agency heads, that embodies these principles. (3-30-01)

07. Physical Security Standards. User agencies will observe standards and procedures to ensure security of the physical premises and computing equipment. The minimum standards and procedures include the following: (3-30-01)

- a.** Access to computer rooms will be limited to staff who require access for the normal performance of their duties. (3-30-01)
- b.** Electrical power protection devices to suppress surges, reduce static, and provide battery backup in the event of a power failure will be used as necessary. (3-30-01)
- c.** Computer system backups shall be stored in a secure location with restricted access. (3-30-01)
- d.** Network infrastructure components will be controlled with access limited to only support personnel with a demonstrated need for access. (3-30-01)
- e.** Physical labeling of infrastructure components will be done to assist in proper identification. Additionally, all components will be inventoried at regular intervals for asset management and physical protection. (3-30-01)

08. Network Security Standards. User agencies shall exercise appropriate security precautions when

connecting ILETS and computer systems linked to ILETS with external untrusted systems. The primary objective of such precautions is to prevent unauthorized access to sensitive information while still allowing authorized users free access. The minimum standards and procedures include the following: (3-30-01)

a. Agencies shall routinely audit for and remove unused or unneeded services/accounts, review accounts periodically, and enforce aggressive and effective password strategies. (3-30-01)

b. Agencies shall ensure that the software security features of the networks they manage are installed and functioning correctly. (3-30-01)

c. Agencies shall monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. (3-30-01)

d. Agencies shall implement and maintain procedures to provide the ILETS network adequate protection from intrusion by external and unauthorized sources. (3-30-01)

e. No computer connected to the network can have stored, on its disk(s) or in memory, information that would permit access to other parts of the network. For example, scripts used in accessing a remote host may not contain passwords. (3-30-01)

f. No connection to ILETS may be established utilizing dial-up communications. Asynchronous communications connections should be limited and tightly controlled as they pose a serious risk because they can circumvent any security precaution enacted to protect networks from untrusted sources. (3-30-01)

g. Network management protocols shall be limited to internal or trusted networks. (3-30-01)

h. Any system having direct or indirect access to the Internet via their computer network shall have in place services that allow no access to ILETS from the Internet. Organizations with large distributed Wide Area Networks connecting many remote sites may choose to incorporate many security layers and a variety of strategies. These strategies shall incorporate the implementation of a firewall to block network traffic, and restriction of remote user access. (3-30-01)

025. -- 027. (RESERVED).

028. USER AGENCY SANCTIONS.

01. Review Of Violations. The board shall review violations of ILETS rules and may impose appropriate sanctions on user agencies. (3-30-01)

02. Objective Of Sanctions. The objectives of the sanction procedure shall be as follows: (3-30-01)

a. To ensure the security, integrity, and financial stability of the ILETS. (3-30-01)

b. To 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 access to its information. (3-30-01)

03. Class Of Sanctions. 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. 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 ILETS data by unauthorized individuals. All other violations are classed as administrative. (3-30-01)

04. Form Of Sanctions. When imposing sanctions, the board shall consider the severity of the violation, the violation type, either administrative or security, and previous sanctions issued, if any. The board may impose as sanctions one (1) or more of the following: (3-30-01)

- a. Written warning. (3-30-01)
- b. Written notice of violation. (3-30-01)
- c. Written notice of probation. (3-30-01)
- d. Written notice of temporary suspension. (3-30-01)
- e. Written notice of permanent suspension. (3-30-01)
- 05. Effective Date Of Sanctions.** 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. (3-30-01)
- 06. Reinstatement.** An agency placed on permanent suspension may apply to the board for reinstatement. (3-30-01)
- 029. -- 999. (RESERVED).**

Subject Index

A

Adjusted Access Fees During Pilot
Projects, ILETS Network 8
Administration Of Criminal Justice 2
Administrative Messages, Information
Access & Dissemination, ILETS 9
Agency Access To ILETS 6
Agency Security Contacts, ILETS
Security 10
Associated System, Accessible Through
ILETS 3
Authorized Agencies, ILETS Access By
Agencies 6

B

Background Checks Of Terminal
Operators Required, Terminal Access
To The ILETS Network 8

C

Criminal History Records, Information
Access & Dissemination, ILETS 8
Criminal Justice Agency 3

D

Definitions, IDAPA 11.10.01, Rules
Governing ILETS - Idaho Law
Enforcement Teletypewriter
System 2
Definitions, ILETS Security 9

E

Effective 12
Establishment, ILETS Network 5
Executive Officer Of The Board,
ILETS 4
Executive Officer, ILETS Board 3

G

General Policy, ILETS Security 9

I

III, Interstate Identification Index 3
ILETS Board 4, 5
ILETS Board, Resignations &
Replacements, Notification 5
ILETS Network 5
ILETS Network User Access Fees 6
ILETS Security 9
ILETS Security Officer 10
ILETS, Idaho Law Enforcement
Teletypewriter System 3
Information Access & Dissemination,
Information Made Available To
ILETS From Various Sources &
Agencies 8

M

Management Control Agreement,

Between Criminal Justice & Non-
Criminal Justice Agency 3
Meetings & Quorum 4

N

NCIC, National Crime Information
Center 4
NLETS, National Law Enforcement
Telecommunication System 4
Non-Criminal Justice Agency 4

P

Payment of Fees Required, User Access
Fees, ILETS Network 6
Physical Security Standards, ILETS
Security 10
Powers & Duties, Chairman, & Ad Hoc
Advisory Committees 5

T

Terminal Agency Coordinators,
Terminal Access To The ILETS
Network 8

U

User Access Fees, ILETS Network 6
User Agency Sanctions, ILETS
Network 11
User Responsibilities, Terminal Access
To The ILETS Network 8