Terri Kondeff
Director

Legislative Services Office
Idaho State Legislature

Serving Idaho's Citizen Legislature

MEMORANDUM

TO: Senators LAKEY, Ricks, Burgoyne and,
Representatives CHANEY, Hartgen, Gannon

FROM: Ryan Bush - Principal Legislative Drafting Attorney

DATE: August 03, 2021

SUBJECT: Temporary Rule

IDAPA 11.10.01 - Notice of Omnibus Rulemaking (Fee Rule) - Adoption of Temporary Rule \ Rescission of Previous Temporary Rule - Docket No. 11-1001-2100F

We are forwarding this temporary rule to you for your information only. No analysis was done by LSO. This rule is posted on our web site. If you have any questions, please call Ryan Bush at the Legislative Services Office at (208) 334-4845. Thank you.

Attachment: Temporary Rule

IDAPA 11 – IDAHO STATE POLICE
IDAHO PUBLIC SAFETY AND SECURITY INFORMATION SYSTEM

DOCKET NO. 11-1001-2100F (FEE RULE)

NOTICE OF OMNIBUS RULEMAKING – ADOPTION OF TEMPORARY RULE \ RESCISSION OF PREVIOUS TEMPORARY RULE

EFFECTIVE DATE: The effective date of the temporary rule being adopted through this omnibus rulemaking as listed in the descriptive summary of this notice is July 1, 2021. The rescission of previous temporary rule under docket 11-1001-2000F is effective July 1, 2021.

AUTHORITY: In compliance with Sections 67-5226, Idaho Code, notice is hereby given this agency has adopted a temporary rule and rescinded a previous temporary rule. The action is authorized pursuant to Section 19-5201 - 5204, Idaho Code.

DESCRIPTIVE SUMMARY: The following is the required finding and concise statement of its supporting reasons for adopting a temporary rule and rescinding a previous temporary rule:

This temporary rulemaking adopts and republishes the following existing rule chapter previously submitted to and reviewed by the Idaho Legislature under IDAPA 11.10, rules of the Idaho Public Safety and Security Information System, known as "ILETS":

IDAPA 11.10
- *11.10.01, Rules Governing Idaho Public Safety and Security Information System.*

ILETS is a dedicated data communication network that links local, state, federal and foreign criminal justice agencies to state records and files, and to the National Crime Information Center (NCIC), which includes criminal history data and files on wanted or missing persons, orders of protection, property and other files critical to criminal justice and public protection. Through ILETS, information and identification services are provided that assist law enforcement agencies to detect and apprehend criminals, promoting public and officer safety, and supporting the criminal justice system in the prosecution, adjudication, and correctional supervision of offenders. This IDAPA rule is necessary to support the operation and connection of ILETS to other state and national criminal history data, provide a vital connection that is not available in any other agency, form, or process. The rescission of previous temporary rule aligns this chapter wholly with the administrative code effective 7-1-21.

TEMPORARY RULE JUSTIFICATION: Pursuant to Sections 67-5226(1)(a-c) and 67-5226(2), Idaho Code, the Governor has found that temporary adoption of the rule is appropriate for the following reasons:

This temporary rule is necessary to protect the public health, safety, and welfare of the citizens of Idaho and confer a benefit on its citizens. The temporary rule implements the duly enacted laws of the state of Idaho, provides citizens with the detailed rules and standards for complying with those laws, and assists in the orderly execution and enforcement of those laws. The expiration of this rule without due consideration and processes would undermine the public health, safety and welfare of the citizens of Idaho and deprive them of the benefit intended by this rule.

FEE SUMMARY: Pursuant to Section 67-5226(2), the Governor has found that the fees or charges being imposed or increased is justified and necessary to avoid immediate danger and the fees are described herein:

The fees or charges, authorized in Section 19-5202(4), Idaho Code, are part of the agency's 2022 budget that relies upon the existence of these fees or charges to meet the state's obligations and provide necessary state services. Failing to reauthorize these temporary rules would create immediate danger to the state budget, immediate danger to necessary state functions and services, and immediate danger of a violation of Idaho's constitutional requirement that it balance its budget. The following is a specific description of the fees or charges:

All law enforcement agencies with a signed user agreement and a direct terminal connection or system access to the ILETS network pay access and usage fees based on that agency's percentage of total annual messages sent and received by the agency through the ILETS message switcher. The total percentage for an agency includes the message traffic generated by any other agency authorized to access ILETS through that agency's direct terminal or system access.

ASSISTANCE ON TECHNICAL QUESTIONS: For assistance on technical questions concerning the adoption of temporary rule and rescission of temporary rule, contact Bureau Chief Leila McNeill, phone (208) 884-7136, fax (208) 884-7193, email Leila.mcneill@isp.idaho.gov.

DATED this 1st day of July, 2021.

Lt. Colonel Bill Gardiner
Chief of Staff
Idaho State Police
700 S. Stratford Dr.
Meridian, Idaho 83642
(208) 884-7004
Bill.Gardiner@isp.idaho.gov

IDAPA 11 – IDAHO STATE POLICE
IDAHO PUBLIC SAFETY AND SECURITY INFORMATION SYSTEM

11.10.01 – RULES GOVERNING IDAHO PUBLIC SAFETY AND SECURITY INFORMATION SYSTEM

000. LEGAL AUTHORITY.
Title 19, Chapter 52, Idaho Code, creates an information system board and authorizes it to make rules necessary to establish and operate the Idaho Public Safety and Security Information System, known as "ILETS." (7-1-21)T

001. SCOPE.
These rules relate to the governance and operation of the Idaho Public Safety and Security Information System. (7-1-21)T

002. INCORPORATION BY REFERENCE.

01. Incorporated Documents. IDAPA 11.10.01 incorporates by reference the full text of the requirements relating to criminal justice information and the system used to transport such information found in the following documents: (7-1-21)T

a. "Criminal Justice Information Systems," 28 CFR Part 20 (July 1, 2006); (7-1-21)T

b. "Criminal Justice Information Systems--CJIS Security Policy," Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, Version 5.8 (June 2019); (7-1-21)T

c. "National Crime Information Center 2000, Operating Manual," Federal Bureau of Investigation, National Crime Information Center (August 2015); (7-1-21)T

d. The International and Public Safety Network, NLETS, Users Guide, (October 19, 2012); (7-1-21)T

e. The International and Public Safety Network, NLETS, Policies and Procedures, (October 19, 2012). (7-1-21)T

02. Document Availability. The above listed documents are available during normal working hours for inspection and copying at the Idaho State Police. (7-1-21)T

003. -- 009. (RESERVED)

010. DEFINITIONS.

01. Access Agency. An agency that electronically accesses ILETS through the services of an interface agency. (7-1-21)T

02. Administration of Criminal Justice. (7-1-21)T

a. Performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. (7-1-21)T

b. It also includes: criminal identification activities; and collection, storage, and dissemination of criminal history record information. (7-1-21)T

03. Associated System. Any automated or manual information system that is accessible through ILETS. (7-1-21)T

04. Board. The Board created by Title 19, Chapter 52, Idaho Code to establish priorities and operational policies and procedures relating to ILETS. (7-1-21)T

05. Criminal Justice Agency. (7-1-21)T

a. Federal and state courts having jurisdiction to hear criminal matters; and (7-1-21)T

b. A government agency or a subunit of a government 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. (7-1-21)T

06. Department. The Idaho State Police, or its successor agency. (7-1-21)T

07. Executive Officer. A position on the ILETS Board filled by the director of the Idaho State Police, or its successor agency. (7-1-21)T

08. 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. (7-1-21)T

09. ILETS. The Idaho Public Safety and Security Information System as established by the director of Idaho State Police pursuant to Title 19, Chapter 52, Idaho Code, includes all hardware, software, electronic switches, peripheral gear, microwave links, and circuitry that comprise the system. (7-1-21)T

10. Interface Agency. An agency that has management control of a computer system directly connected to ILETS. (7-1-21)T

11. 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 gives the criminal justice agency authority to set and enforce policies governing the non-criminal justice agency's access to ILETS. (7-1-21)T

12. NCIC 2000. The Federal Bureau of Investigation National Crime Information Center, is a computerized information system that includes telecommunications lines and 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. (7-1-21)T

13. NLETS. The International Justice and Public Safety Information Sharing Network, is a national computerized message switching system that links national and state criminal justice information systems. (7-1-21)T

14. 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. (7-1-21)T

011. (RESERVED)

012. EXECUTIVE OFFICER OF THE BOARD.

01. Authority of Office. The executive officer represents 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 executes instruments for, and on behalf of, the Board and ILETS. (7-1-21)T

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: (7-1-21)T

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 (7-1-21)T

b. Management and safekeeping of all documents relating to the Board and ILETS operations. (7-1-21)T

013. ILETS BOARD: MEETINGS AND QUORUM.

01. Schedule of Meetings. The Board holds regular meetings 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. (7-1-21)T

02. Quorum. When meeting, four (4) members of the Board constitutes a quorum necessary for transacting business. (7-1-21)T

03. Representation at Meetings. A board member may appoint a proxy to attend a meeting and exercise the voting privilege of that member. (7-1-21)T

a. An Idaho State Police proxy must be at least a major in rank; (7-1-21)T

b. A police chief proxy must be an Idaho police chief; (7-1-21)T

c. A sheriff proxy must be an Idaho sheriff; and (7-1-21)T

d. Proxy designations must be made in writing to the Executive Officer prior to the meeting. (7-1-21)T

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 enforces compliance with all laws and regulations governing ILETS operations. (7-1-21)T

02. Election of Chairman. At the first regular meeting of a calendar year, the Board elects a chairman from its membership by majority vote. The chairman serves a term of one (1) year and may succeed himself. (7-1-21)T

03. Presiding Officer. The chairman presides at all meetings and conduct the meetings pursuant to "Roberts' Rules of Order, Current Revised Edition." If the chairman is absent from a meeting, the executive officer presides at that meeting. (7-1-21)T

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. (7-1-21)T

015. (RESERVED)

016. ILETS NETWORK.

01. Establishment. The executive officer establishes ILETS as a program of the Idaho State Police or its successor agency. (7-1-21)T

02. Responsibilities. The program, as established by the executive officer, has the following responsibilities: (7-1-21)T

a. Develop and operate a computerized criminal justice telecommunications and information system that provides message switching and record inquiry and retrieval capabilities. (7-1-21)T

b. Publish an ILETS Operations Manual and distribute copies to each user agency. (7-1-21)T

c. Function as the NCIC control terminal agency and the NLETS control terminal agency for the State of Idaho. (7-1-21)T

d. Assist and train criminal justice agencies regarding information retrieved from ILETS and

associated systems for use in administration of criminal justice. (7-1-21)T

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. (7-1-21)T

f. Provide staff support to the ILETS Board. (7-1-21)T

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. (7-1-21)T

h. Create model management control agreements between criminal justice agencies and non-criminal justice agencies. (7-1-21)T

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. (7-1-21)T

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 is restricted to the following governmental agencies: (7-1-21)T

a. Criminal justice agencies; (7-1-21)T

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; (7-1-21)T

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 (7-1-21)T

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. (7-1-21)T

02. Management Control Agreements. The management control agreement between a criminal justice agency and a non-criminal justice agency grants to the criminal justice agency the authority to set and enforce: (7-1-21)T

a. Priorities of service; (7-1-21)T

b. Standards for the selection, supervision, and termination of personnel authorized to access ILETS; and (7-1-21)T

c. Policies governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit information to or receive information from ILETS. (7-1-21)T

03. Board Approval. The Board reviews all requests for access to ILETS and determines 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. (7-1-21)T

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. (7-1-21)T

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: (7-1-21)T

a. An agency at the county or municipal level pays an annual access fee of five thousand dollars ($5,000). (7-1-21)T

b. An agency at the state, federal, or tribal level pays an annual access fee of eight thousand, seven hundred fifty dollars ($8,750). (7-1-21)T

03. Usage Fee. Any agency that has signed a user agreement with ILETS to have direct terminal or system access to the ILETS network pays 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 includes the message traffic generated by any other agency authorized to access ILETS through that agency's direct terminal or system access. (7-1-21)T

a. The usage fee is assessed according to the following schedule:

Percentage of Total ILETS Message Traffic	Annual Usage Fee Effective October 1, 2014
0 - .25 %	$1,875
.26 - .50 %	$3,750
.51 - .75 %	$7,500
.76 - 1.0 %	$15,000
1.01 - 1.50 %	$22,500
1.51 – 2.0 %	$33,750
2.01 – 5.0 %	$50,625
> 5.01 %	$75,939

(7-1-21)T

b. The department will conduct audits of ILETS message switcher traffic for even-numbered years to determine an agency's annual usage fee. This fee is effective for two (2) years and begins with the quarterly statement beginning October 1 of odd-numbered years. (7-1-21)T

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 will be adjusted to reflect the combined historical usage. (7-1-21)T

d. A new agency approved for direct ILETS access that does not have historical usage will be assessed an interim usage fee by the department pending the next audit of ILETS message traffic. The department sets an interim fee based on the agency's similarities to existing agencies with direct terminal or system access. An agency may appeal the interim usage fee set by the department to the ILETS Board. (7-1-21)T

e. As operator of ILETS, the department, in lieu of payment of fees, provides direct and in-kind support of network operations. The Board reviews biennially the proportion of that support to the overall operating cost of the system. (7-1-21)T

04. Billing and Payment. The department mails 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. (7-1-21)T

05. Sanctions for Delinquency. Any user agency that becomes delinquent in payment of assessed fees is subject to sanctions under Section 028. (7-1-21)T

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 is based on any cost savings, actual or anticipated, realized by the ILETS network. (7-1-21)T

020. USER RESPONSIBILITIES.

01. User Agreement. Any agency with access to 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 or an interface agency to that effect. (7-1-21)T

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 be on file for review during an ILETS or NCIC audit. When the agency has completed the validation process, the records must be modified to verify their validity no later than thirty (30) days after receiving electronic notification. (7-1-21)T

03. Minimum Training. Each agency employee who operates a computer to access ILETS must complete ILETS training at a level consistent with the employee's duties. Each employee who operates a computer to access ILETS must be re-certified by the agency every two (2) years. (7-1-21)T

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 that indicates the status of the record or a time frame when the record status will be confirmed. (7-1-21)T

05. Terminal Agency Coordinators. The agency administrator of each agency with computer access to ILETS must designate one (1) or more terminal agency coordinators who will be the primary contact(s) for all matters relating to use of ILETS by the agency. A terminal agency coordinator must have sufficient authority to implement and enforce necessary policy and procedures. (7-1-21)T

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 NCIC background screening policies are also adopted for all ILETS access. (7-1-21)T

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. (7-1-21)T

02. Criminal History Records. Criminal history information accessed via ILETS from a state or national computerized file is 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. (7-1-21)T

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 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: (7-1-21)T

a. No messages supportive or in opposition to political issues, labor management issues, or announcements of meetings relative to such issues. (7-1-21)T

b. No messages supportive or in opposition of legislative bills. (7-1-21)T

c. No requests for criminal history record information. (7-1-21)T

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 accessing ILETS directly, or another system that has access to the ILETS network, to implement the procedures necessary to make the access device secure from any unauthorized use and to ensure ILETS is not subject to a malicious disruption of service. ILETS access agencies must 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 an access agency or network connection when serious security threats and vulnerabilities are detected. (7-1-21)T

02. Definitions. The following is a list of terms and their meanings as used in the ILETS security rule: (7-1-21)T

a. Computer interface capabilities means any communication to ILETS allowing an agency to participate in the system. (7-1-21)T

b. Firewall means a collection of components placed between two (2) networks that keep the host network secure by having the following properties: (7-1-21)T

i. All traffic from inside the network to outside, and vice-versa, must pass through it; (7-1-21)T

ii. Only authorized traffic is allowed to pass; and (7-1-21)T

iii. The components as a whole are immune to unauthorized penetration and disablement. (7-1-21)T

c. ILETS Security Officer (ISO) is the department staff member designated by the executive officer to monitor and enforce agency compliance with site and network security requirements. (7-1-21)T

d. Peer networks are computer interfaces between cooperative governmental agencies in Idaho where none of the participating entities exercise administrative or management control over any other participating entity. (7-1-21)T

e. Interface agency is an agency that has management control of a computer system directly connected to ILETS. (7-1-21)T

f. Untrusted system is a system that does not employ sufficient hardware or software security measures to allow its use for simultaneously processing a range of sensitive or confidential information. (7-1-21)T

03. Interface Agency 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 Interface Agency Addendum must exist between ILETS and all interface agencies. This agreement will clarify that the interface agency is equally responsible for actions by secondary and affiliated systems connected through their site to ILETS. Interface agencies must put in place similar subsidiary security agreements with secondary and affiliated systems to protect its network and ILETS. (7-1-21)T

04. ILETS Security Officer. The ILETS Security Officer is responsible for the following duties: (7-1-21)T

a. Disseminating to user agencies copies of ILETS security policies and guidelines; (7-1-21)T

b. Communicating to user agencies information regarding current perceived security threats and providing recommended measures to address the threats; (7-1-21)T

c. Monitoring use of the ILETS network either in response to information about a specific threat, or generally because of a perceived situation; (7-1-21)T

d. Directing an interface agency, through its nominated contact, to rectify any omission in its duty of responsibility; (7-1-21)T

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 (7-1-21)T

f. Provide support and coordination for investigations into breaches of security. (7-1-21)T

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. (7-1-21)T

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 an interface agency, signed by the agency heads, that embodies these principles. (7-1-21)T

07. Physical Security Standards. Interface agencies will observe standards and procedures to ensure security of the physical premises and computing equipment. The minimum standards and procedures include the following: (7-1-21)T

a. Access to computer rooms will be limited to staff who require access for the normal performance of their duties. (7-1-21)T

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. (7-1-21)T

c. Computer system backups shall be stored in a secure location with restricted access. (7-1-21)T

d. Network infrastructure components will be controlled with access limited to support personnel with a demonstrated need for access. (7-1-21)T

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.

(7-1-21)T

f. An interface agency must create and enforce a password policy in which the agency is responsible for assigning ILETS users a unique password. The password policy must require that a new password be initiated by the user or agency every ninety (90) days. (7-1-21)T

08. Network Security Standards. User agencies must 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: (7-1-21)T

a. Agencies must routinely audit for and remove unused or unneeded services/accounts, review accounts periodically, and enforce aggressive and effective password strategies. (7-1-21)T

b. Agencies must ensure that the software security features of the networks they manage are installed and functioning correctly. (7-1-21)T

c. Agencies must monitor network security on a regular basis. Adequate information concerning network traffic and activity must be logged to ensure that breaches in network security can be detected. (7-1-21)T

d. Agencies must implement and maintain procedures to provide the ILETS network adequate protection from intrusion by external and unauthorized sources. (7-1-21)T

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. (7-1-21)T

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. (7-1-21)T

g. Network management protocols must be limited to internal or trusted networks. (7-1-21)T

h. Any system having direct or indirect access to the Internet via their computer network must 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 must incorporate the implementation of a firewall to block network traffic, and restriction of remote user access. (7-1-21)T

i. Agencies accessing ILETS directly or through another agency, must insure that all telecommunications infrastructure meets the FBI CJIS Security Policy for encryption standards. (7-1-21)T

j. No routing or IP Network Translations are to be performed on individual access devices. All routing and translation must be performed on a router or firewall device. (7-1-21)T

025. -- 027. (RESERVED)

028. USER AGENCY SANCTIONS.

01. Review of Violations. The board reviews violations of ILETS rules and may impose appropriate sanctions on access agencies. (7-1-21)T

02. Objective of Sanctions. The objectives of the sanction procedure are as follows: (7-1-21)T

a. To ensure the security, integrity, and financial stability of the ILETS. (7-1-21)T

b. To create an awareness among access 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. (7-1-21)T

03. Class of Sanctions. Sanctions are 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 are classed as either administrative (minor) or security (serious) violations. Security violations are defined as ones which have or could result in access of ILETS data by unauthorized individuals. All other violations are classed as administrative. (7-1-21)T

04. Form of Sanctions. When imposing sanctions, the Board considers the severity of the violation, the violation type, either administrative or security, and previous sanctions issued. The Board may require the violating agency to submit a mediation plan showing how the violation will be corrected and future violations prevented. The Board shall consider such a mediation plan, if submitted, when imposing sanctions. The Board may impose as sanctions one (1) or more of the following: (7-1-21)T

a. Written warning. (7-1-21)T

b. Written notice of violation. (7-1-21)T

c. Written notice of probation. (7-1-21)T

d. Written notice of temporary suspension. (7-1-21)T

e. Written notice of permanent suspension. (7-1-21)T

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. (7-1-21)T

06. Reinstatement. An agency placed on permanent suspension may apply to the Board for reinstatement. (7-1-21)T

029. -- 999. (RESERVED)