B. COMPUTER USE

PURPOSE

The availability and use of the computer within the work environment has provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on the Greater Lafourche Port Commission, its members, and the public if not managed properly. Therefore, it is the policy of the Greater Lafourche Port Commission that all members abide by the guidelines set forth herein when using computers and the services for both internal and external databases and information exchange networks, and where applicable, voice mail, mobile data terminals, and related electronic messaging devices. It is the purpose of this policy to provide employees with guidance on the proper use of agency owned computers and related electronic messaging systems. This equipment is utilized within the Greater Lafourche Port Commission for purposes of writing reports, record management, disseminating electronic mail, utilizing services of the Internet, and related electronic message transmissions, recording, storage, and access to the Integrated Criminal Information Justice System (ICJIS) and the Criminal Justice Information System (CJIS).

All employees of the Greater Lafourche Port Commission shall heed to the policies listed below and all other policies and regulations governing the National Crime Information Center (NCIC) as set forth by the Criminal Justice Information Services (CJIS).

SCOPE

This policy applies to all permanent, probationary, provisional, temporary, part-time, classified, unclassified and non-Civil Service employees.

DEFINITIONS

1. Electronic Messaging Device - for the purpose of this policy, electronic messaging devices include personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards, internet services, mobile data terminals, and facsimile transmissions.

2. Hardware — the physical components of a computer system (central processor, memory, disk drives, printer, monitor, computer boards, peripherals, etc.)

3. Information Systems Division Work Order System – a form used to submit needed computer services. This includes software requests, programming, website request, equipment repair, user access, modifications, computer or network problems or other assistance.

4. Information System Administrator (IT Administrator) - for the purpose of this policy, the member of the Greater Lafourche Port Commission designated with the responsibility for managing the agency's LAN/WAN and all aspects of electronic messaging through individual computers and computer networks within this agency.

5. Microcomputer - a complete small computing system with the capability to run programs and store data.

6. Mobile Data Terminal – (MDT) a mobile computer such as a laptop.

7. Software - instructions and programs that tell the computer what operations to perform.

8. Unauthorized Access - signing on to any system other than the specific systems, which have been defined as necessary to fulfill the functions of the employee's current job assignment. This inc1udes trying to change records through unauthorized screens or accessing unauthorized systems.

9. Wide Area Network (WAN) - a network that extends across cities, states, or continents.

10. Local Area Network (LAN) - a system allowing several concentrations of computers within a local area to share resources, such as peripherals, software, or data.

11. Wallpaper – wallpaper is the monitor pattern or picture or other graphic representation that forms the background onto which all the icons, menus, and other elements of Windows XP are displayed and moved around.

12. Web Browser - a software application used to locate and display Web Pages. (Examples: Microsoft Internet Explorer – Netscape Navigator)

13. Internet Explorer Home Page - The main page of the internet when the Internet Explorer Browser is opened.

14. Screensaver - A small program that takes over the display screen if there are no keystrokes or mouse movements for a specified duration.

15. Default - A value or setting that a device or program automatically selects if you do not specify a substitute.

16. Integrated Criminal Information Justice System (ICJIS) - provides real-time access to information. It translates information from one data source to another and integrates information to form a complete picture. This process allows different agencies to access needed data to do their job, but maintains secure control over their own data.

17. Criminal Justice Information Services (CJIS) - the focal point and central repository for criminal justice information services in the Federal Bureau of Investigations. Timely and relevant criminal justice information is made available to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations, and activities, and other law enforcement related data.

18. Louisiana Law Enforcement Telecommunications System (LLETS) - is a computer network which allows connectivity and communication with various criminal justice databases by using what is commonly referred to as a "message switch".

19. National Crime Information Center (NCIC) – is a nationwide, computerized information system established as a service to all criminal justice agencies – local, state, and federal.

20. Thinkstream – is a web interface used to access ICJIS, CJIS, LLETS, and NCIC as well as other databases as they come online.

21. Terminal Agency Coordinator (TAC) – is the agency liaison for Thinkstream, CJIS, LLETS, NCIC, and ICJIS.

POLICY

1. Security

a. Computer system security is, generally, divided into two distinct types, physical security and logical security. Physical security depends on unauthorized persons not being able to physically reach a computer terminal or having the keyboard locked in such a manner to prohibit them from issuing commands to the computer. Logical security involves the use of various passwords and key phrases to block access to systems for which a user's need has not been proven, and authorization has not been approved. Microcomputers use a combination of both types of security.

b. All personnel who have access to the LAN/WAN will be provided with a "Login" name and will be required to use only their login when signing onto the system. Personnel will only use the Login that has been provided to them by the IT Administrator and are strictly prohibited from creating secret passwords or any other type of locking system to prevent others from using a specific workstation. The IT Administrator on a case-by-case basis may grant exceptions to this rule.

c. Choosing a password provides login security, which protects the data on the computer network.

i. A password may be created or changed with a minimum of six (6) characters. Do not use punctuation characters (!#$ %%&*O_+?><) as part of a password. Passwords can be up to 128 characters long. A unique password must be entered to login to the network. All passwords must contain at least one numeral within it.

ii. Passwords should be difficult for unauthorized users to decipher. The use of names of children, pets, spouses, favorite teams, favorite band, phone number, and anniversary, etc. is discouraged.

iii. The microcomputer system will force password changes every 120 days. In the event of a lock out, contact the IT Administrator for assistance.

iv. To help prevent corruption of data in network files and unauthorized users from accessing restricted files, passwords are not to be given to unauthorized users. Individual users are responsible for actions performed under their login ID and password.

v. If there is a suspicion that an unauthorized user has learned and has been using another individual's assigned password, a new password should be entered. The user shall notify the IT Administrator immediately if this occurs.

vi. When an employee changes their password, the new password should be sent to the IT Administrator. There are certain programs that only the Computer System Administrator can change. Failure to send this password may cause you to be locked out of certain programs such as the ICJIS program. Employees should be only changing passwords for their logon to the network and not for their logon to, Thinkstream, Accounting Software, or other applications that require a separate password.

d. The Human Resource Division, using the Wide Area Network or public service, shall notify the IT Administrator immediately upon the determination that an employee is to be dismissed or is resigning. In addition, when an employee is transferred, IT Administrator should be notified so that appropriate access may be given for the new assignment and removed from the old assignment.

e. Any employee found making unauthorized access to any computer application shall be subject to disciplinary actions up to and including dismissal. Unauthorized access to the computer systems constitutes a danger to the Parish of Lafourche due to the sensitive nature of information contained in its computer systems, as well as a loss of productive time while employees are accessing systems where they have no authorization.

f. A Greater Lafourche Port Commission network computer should never be connected to a public bulletin board or chat rooms without proper authorization and security briefing by the IT Administrator. Public

bulletin boards create a liability for unauthorized non-employees access and virus penetration.

g. Use of the Internet, Intranet, & mail and their related resources is designated for official Greater Lafourche Port Commission business. Transmission of electronic messages and information on communications media provided for employees of the Greater Lafourche Port Commission shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence.

h. Electronic Messaging Devices and their contents, with the exception of personally owned software authorized for installation on agency computers, are the property of the Greater Lafourche Port Commission and intended for use in conducting official business, with limited exceptions noted elsewhere in this policy.

i. Employees are advised that they do not maintain any right to privacy in electronic messaging device equipment or its content, to include personally owned software.

   i. E-mail is the property of the Greater Lafourche Port Commission. Any E-mail (including personal) constitutes an official Greater Lafourche Port Commission Office document. It is subject to inspection at any time. This material is fully discoverable by most courts in addition to internal inquiries.
   ii. The Greater Lafourche Port Commission reserves the right to access any information contained in electronic messaging devices and may require members to provide password(s) to files that have been encrypted or password protected.
   iii. The Greater Lafourche Port Commission reserves the right to access, for quality control purposes and/or for violations of this policy, electronic and voice transmissions of members conducting agency business.

j. No member shall access or allow others to access any file or database unless that person has a need and right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

k. Accessing or transmitting materials, other than that required for law-enforcement business, involving the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

l. The computers are to be used for Greater Lafourche Port Commission business only. An audit of computer use may take place at any time. Any personal material found on computers will be erased immediately, such as computer games, indecent material, and personal documents.

m. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or network systems) only to individuals with a need and right to know and where there is sufficient assurance that appropriate security of such information will be maintained. Such information includes, but is not limited to the following:

i. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.
ii. Criminal history information and confidential informant files, identification files, or related information.
iii. Intelligence files and information containing sensitive tactical and undercover information.

2. Computer Operations Help Desk and Assistance

a. Request for computer services shall be made to the IT Administrator.

i. A Work Order Form shall be completed and emailed by the employee to the IT Administrator for the purposes of tracking specific computer problems and to ensure that your problem is resolved in a timely manner. In the event email doesn't work, then a phone call to the IT Administrator should be placed explaining the problem with as much detail as possible.
ii. Employees shall furnish as much information as possible to the IT Administrator to insure timely resolution. For example: If there is an error message that showed up on your computer screen we need to know exactly what the error message says.
iii. The Work Order shall be prioritized by IT Administrator.
iv. After the Work Order has been reviewed by IT Administrator, an email will be sent to employee with an estimated time of resolution.
v. In the event changes to a network or workstation are required, such as location, software, hardware, user logins, etc., a request shall be submitted to the IT Administrator via Work Order Form or Phone call.
vi. All software must be approved by the IT Administrator and shall be loaded onto the system by IT Administrator or his/her designee only.

vii. Any computer or computer equipment that is malfunctioning shall be reported immediately to the IT Administrator via Work Order Form or Phone Call. Personnel shall not:
    1. Tamper with network or routing devices,
    2. Remove, disconnect, or uncouple any wires or cables,
    3. Remove cover from computer or attempt to fix computer, or
    4. Hit or strike computer in any way.

viii. Only IT Administrator or his/her designees may relocate a computer. The computers may not be taken home or reassigned, without approval of IT Administrator.

ix. Users shall log off their computers before leaving for the day, leaving the computer on. Monitors shall be turned off when leaving.

x. Employees should use extreme caution when eating or drinking at a computer workstation. In the event any liquid is spilled on the

xi. computer system, the user should:
    1. Logout immediately,
    2. Turn off all power to the system,
    3. Wipe up the spill quickly, and
    4. Advise the IT Administrator.

xii. If a problem occurs with the system during non-business hours, notify IT Administrator via Work Order Form and email. If the problem is such that it will require immediate attention or email is the problem, the IT Administrator shall be contacted via telephone.

3. Computer Software and Hardware Needs

a. The IT Administrator shall, as deemed necessary, evaluate the needs of the agency for computer based services. This evaluation will take place prior to the start of the budget process and will include any additional software/hardware needs. The IT Administrator will conduct a survey of the LAN/WAN users as a part of this evaluation and will submit to the Department head a budget request covering the department needs.

b. Microcomputers are installed and are in use throughout the Greater Lafourche Port Commission to provide efficiency through automation. Only hardware and software owned by or under contract to the Greater Lafourche Port Commission is authorized for use within this agency. All authorized hardware and software shall be installed and maintained by or under the direction of the IT Administrator. Employees of the Greater Lafourche Port Commission shall not use unauthorized hardware or software in the performance of official duties. Software games are not authorized to be installed in any agency owned computers. To request a software installation, users must submit a request to the IT Administrator via Work Order Form, along with a copy of the software and ownership documentation.

4. Default Workstation and MDT Desktop Settings:

a. The Wallpaper will be that of the official Greater Lafourche Port Commission Logo and installed by the IT Administrator.

b. The Homepage in Internet Explorer shall be www.portfourchon.com.

c. The Screensaver will be that of images of the Greater Lafourche Port Commission and installed by IT Administrator.

d. The IT Administrator at any time discovers that the defaults have been changed to a Workstation or MDT, he/she will reset to the default.

e. Personnel in violation of this policy shall receive the following discipline:

1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense — Corrective Review/Suspension
4th Offense — Corrective/Termination

5. E-mail Communications

The Board of Commissioners of the Greater Lafourche Port Commission establishes this policy for the use of its internal electronic communication "E-mail" system in order to prevent: misuse that can result in message overload; disruption of work performed by computer-network users; inadequate message security; and inappropriate communication that may compromise the Port in subsequent litigation.

a. All members of the Greater Lafourche Port Commission will have an Internet and Intranet E-mai1 address. The IT Administrator will be directed to make the necessary provisions to allow for such access. Violations of E-mai1 access rules will result in the elimination of E-mail access by the offending member as well as appropriate disciplinary action.

b. This policy serves to notify employees of the following:

i. The contents of E-mail messages may be subject to subpoena in legal proceedings and may be requested under public records laws;
ii. E-mail messages are stored on backup tapes for retention;
iii. Employees have no expectation of privacy with E-mail communication and should use the Port's E-mail system accordingly.

iv. The Port regards E-mail as a form of communication which is designed to enhance productivity to accomplish the Port's mission. The Port expects its employees to use the E-mail system primarily for work-related messages. E-mail of a private, personal, or non-work-related nature should be kept to a minimum. E-mail communication is an employee privilege. Employees are expected to use the system responsibly, thoughtfully, and in a professional manner. Employees shall not permit unauthorized persons to use this agency's electronic mail system.

v. The Port's E-mail system is the property of the Port. Messages sent over the E-mail system are also the property of the Port and are subject to monitoring. The Port's management reserves the right to intercept, review, and audit all messages sent over its E-mail system.

c. E-mail may be used for the following purposes:

i. Department activities and/or correspondence;
ii. Personal activities and/or correspondence within reason and as long as all appropriate rules are followed;
iii. A substitute for internal telephone usage, the difference being that an E-mail message can be printed and retained by the recipient and the Port.
iv. Courtesy correspondence for staff members; and
v. Other correspondence as assigned.

d. E-mail shall not be used for or in the following manner:

i. E-mail should not take the place of official memoranda. Formal documentation of Port transactions or policy guidelines or directives should be transmitted by printed memoranda rather than by E-mail.
ii. Any messages involving a potential claim, a claim, or litigation where the attorney/client privilege is a consideration should not be communicated by E-mail.
iii. The use of the Port's E-mail system for unlawful, defamatory, discriminatory or obscene communication is prohibited. Violators of this policy shall be subject to appropriate disciplinary action up to removal from their positions.

The Port will use the reasonable person standard in determining what communication is appropriate. The types of E-mail communication prohibited by this policy include, but are not limited to, messages that:

1. Violate Federal or State laws and/or accepted business or employment practices;
2. Intimidate, abuse, harass, or threaten the receiver or may be perceived as doing so by the receiver;

3. Degrade or insult an individual or a group or serve to malign an individual or a group; or
4. Discuss unlawful practices, activities, material, or information.
5. In addition, non-work-related E-mail messages for which the length and/or frequency impair the productivity of an employee or the efficient operation of a work unit are prohibited.
6. The posting of any correspondence deemed inappropriate to include, but not limited to, material containing references of a sexually explicit or implicit nature, profane or vulgar language, language of a racist nature or derogatory to persons based on race, sex, ethnicity, or sexual orientation;
7. For purposes of commerce, secondary employment, or solicitation;
8. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

iv. Members who have an assigned E-mail address shall attempt to check for incoming messages at the beginning of each workday (at a minimum). Additionally, it is suggested that E-mail boxes should be checked on a regular basis based on anticipated volume of incoming E-mail.

v. An Electronic Messaging Device is designed and intended to conduct business of this agency and is restricted to that purpose. Installation of, or access to, software purely for entertainment purposes is prohibited.

vi. Exceptions to business use include the following:
1. Infrequent personal use of these devices may be permissible if limited in scope and frequency.
2. Personnel may make off-duty use of agency owned computers for professional and career development purposes in keeping with other provisions of the Policy and Procedure Manual.

e. Personnel in violation of this policy shall receive the following discipline:

1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense — Corrective Review/Suspension
4th Offense — Corrective/Termination

6. Internet Use

The Greater Lafourche Port Commission encourages authorized and trained personnel with access to Electronic Messaging Devices to utilize these devices

whenever necessary. However, use of any of these devices is a privilege that is subject to revocation.

The Internet is a constantly-changing, ever-increasing, interconnection of thousands of computer networks throughout the world, bringing new opportunities for conducting business and communication. Internet tools and networking technology are evolving as predominant facilitators of the communication process on a global scale, and their importance, relevance, and impact cannot be ignored.

This policy and these procedures have been developed to establish implementation standards and guidelines for acquiring access to and acceptable use of Internet resources by Port employees.

a. General guidelines for Internet access:

   i. Software supporting Internet access will be installed only by the Port's IT Administrator or his/her designee.
   ii. On all Port computers, all Internet access must be via the Port's Internet link using an authorized Port account. Personal Internet accounts are not permitted.
   iii. When an employee connects to the Internet using the Port's Internet link, it should be used primarily for business-related activity. Personal use should be kept to a minimum and must not incur additional Port expense or interfere with Port business.
   iv. All use of the Internet via Port resources must adhere to all federal, state, and local laws, and all Port policies.
   v. The only Web Browser that will be supported by the IT Administrator will be Internet Explorer unless or until determined by IT Administrator that this is no longer the appropriate browser to access the internet.

b. Employees are prohibited from using the Internet for any use other than for a legitimate business-related purpose of the Greater Lafourche Port Commission. Examples of prohibited use are:

   i. Inquiries or entry into any area where the prevailing topic is sex, sexual conduct, sexually graphic images or similar subject matter, except in the course of a criminal investigation.
   ii. Inquiries or entry into any area where the prevailing topic is related to the practice, purpose, dissemination, or degradation of persons based on the status of race, sex, religion, ethnicity, or sexual orientation, except in the course of a criminal investigation.

iii. Inquiries or entry into any area where the prevailing topic is related to anti-governmental groups, anti-governmental activities, terrorist groups, or similar subject matter, except in the course of a criminal investigation.
iv. Personal gain or profit;
v. To represent yourself as someone else;
vi. Solicitation of Commission employees;
vii. To provide confidential information about Port employees to others;
viii. Commercial solicitations of non-Port business enterprises;
ix. When it interferes with an employee's job or the jobs of other employees;
x. When it interferes with the operation of other Port computers and telecommunications systems;
xi. To view or obtain text or pictorial pornography or the transmission of obscene or harassing messages to any other individual.

c. Examples of acceptable uses of Internet access include:

i. Exchanging E-mail with other Port and outside organizations available through the Internet mail gateway.
ii. Gaining access to and exchanging information quickly and conveniently.
iii. Gaining access to experienced and expert individuals in thousands of fields.
iv. Receiving regular updates on topics of interest relative to one's job function.
v. Translating and transferring data between dissimilar machines.
vi. Building teams and enhancing teamwork.

d. Personnel in violation of this policy shall receive the following discipline:

1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense — Corrective Review/Suspension
4th Offense — Corrective/Termination

7. System Monitoring

A wide variety of information exists on the internet. The Port will employ the use of monitoring software that will capture and report the type of information being accessed and the duration of access of each user. These reports will be available for management review.

8. Downloads:

Individual users must be aware of, and at all times attempt to, prevent the downloading of information that may contain viruses. At a minimum, this can be accomplished by knowing the source of the information being downloaded; and performing frequent backups of data files, and critical information, using anti-virus software.

9. Internet Programming and Application and Development:

As Board presence on the Internet expands, care must be taken to ensure that well-structured and consistent procedures are in place for web page development and maintenance. Therefore, the Port's IT Administrator is the authority for all programming and development and must review and approve all Work Order request for legitimate and mission-related Port business to be published on the website. The approved Work Order is forwarded to the Port's webmaster for his/her input. Once Work Order is approved by both IT Administrator and Webmaster, then it is forwarded to Executive Director for his/her approval. Once approved by Executive Director, Webmaster is responsible for publishing on the Port's Official Website.

The Greater Lafourche Port Commission's Official website is located at www.portfourchon.com.

The following guidelines apply to all web pages:

a. The official website of the Greater Lafourche Port Commission will be updated and maintained by IT Administrator, webmaster, or his/her designee.

b. No personal Web Home Pages are allowed.

c. Personnel in violation of this policy shall receive the following discipline:

1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling

3rd Offense - Corrective Review/Suspension
4th Offense - Corrective/Termination

10. Importing/Downloading Information and Software

a. Members shall not download or install on any Greater Lafourche Port Commission or network terminal any file (including sound and video files attached to e-mail messages unless necessary to do his/her job and the source is known), software, or other materials from the internet or other external source without submitting a Work Order Form to the IT Administrator and receiving authorization.

b. Members shall observe the copyright and licensing restriction on all software applications and shall not copy software from internal and external sources unless legally authorized.

c. Any software for which proof of licensing (original discs, original manuals and/or license) cannot be provided is subject to removal by authorized agency personnel.

d. Privately owned software may be loaded on agency computers if approved by IT Administrator.

e. Privately owned software might be removed if it conflicts with agency hardware or software, interferes with the ability of other members to access or utilize the electronic messaging device, or occupies excessive storage space needed by the agency.

f. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.

g. Any hardware enhancements or additions to Greater Lafourche Port Commission equipment must be approved and authorized by IT Administrator. The IT Administrator is responsible for determining proper installation procedures.

h. To avoid breaches of security, members shall lock or log off his/her Workstation or Mobile Data Terminal (MDT) that has access to the agency's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their Workstation or mobile data terminal.

i. Members who violate this policy or related policies may be held liable for all civil actions. Members may also be subject to disciplinary action, which could include termination of employment. If expenses are incurred to return the computer equipment to its original state of

operation, the employee may be required to reimburse the Greater Lafourche Port Commission.

j. Personnel in violation of this policy shall receive the following discipline:

1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense — Corrective Review/Suspension
4th Offense — Corrective/Termination

11. National Criminal Information Center (NCIC) Authorization and Integrated Criminal Information Justice System (ICJIS) Authorization

a. Only employees certified by the Greater Lafourche Port Commission Terminal Agency Coordinator (TAC) shall be granted access to the NCIC Query program, ICJIS.

b. In order for an employee to be NCIC certified, a test as provided by the State of Louisiana shall be successfully completed. The test results and two fingerprint cards shall be submitted and approved by the State of Louisiana. The agency TAC shall assure submissions are received by the State.

c. When the TAC has received authorization from the state that the employee has been accepted, the TAC shall notify Lafourche Parish Sheriff's Office and LA State Police. The TAC will notify the employee by email once access has been set up.

d. NCIC queries are for law enforcement use only. Personal use of the system shall not be tolerated. A log is maintained of all inquiries by username. Information shall not be disseminated to non-law enforcement agencies or persons. To prevent unauthorized users from accessing restricted files, passwords are not to be given to unauthorized users. Individual users are responsible for actions performed under their login identification (ID) and password.

e. Each user is assigned an ORI number, with user name and password. This ORI number allows for an audit trail of each user and his/her inquiries into the NCIC database.

f. Disciplinary action shall be required for any employee of the Greater Lafourche Port Commission who fails to comply with policies and regulations of the NCIC. In the event of the following violations the appropriate disciplinary actions shall proceed.

g. Security of Terminal - Computer sites shall be in secure locations to protect against any unauthorized viewing or access to computer terminals, access devices, or stored/printed data at all times. Authorized personnel shall accompany all visitors to these locations at all times.

i. Allowing access to unauthorized personnel shall result in the following;
1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense - Corrective Review/Suspension
4th Offense - Corrective/Termination

h. Security of System- Unauthorized personnel are prohibited from modification or destruction of system data, loss of computer system processing capability, or loss by theft of any computer system media including Chip ROM memory, optical or magnetic storage medium, and hardcopy printout etc. This includes, but not limited to the use of floppy discs, downloading programs, playing games, and anything, which may hinder configuration of the system.

i. Destruction of the system in any form shall result in the following;
1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense - Corrective Review/Suspension
4th Offense - Corrective/Termination

i. Certification —All Inquiry Only Operators shall successfully compete the test for certification on an as needed basis. All operators shall follow certification standards as adopted by the State of Louisiana, which is the Louisiana Law Enforcement Telecommunications System (LLETS) Operator Certification Plan. Recertification shall be administered to all operators every two (2) years as set forth by the State of Louisiana and on dates made available by the TAC.

i. Failure to successfully complete the certification or recertification test within the appropriate time limit may result in;
1st Offense - Corrective Review/Counseling and afforded the opportunity to re-test within fifteen days
2nd Offense - Corrective Review/One day suspension and afforded the opportunity to re-test within fifteen days.
3rd Offense - Corrective Review/Termination

j. Inquiry-Only Operators - All operators must be trained and certified. Only certified operators or operators who have been granted temporary access shall operate these terminals. Each operator shall follow certification standards as adopted by the State of Louisiana, which is the LLETS Operator Certification Plan.

i. Non-certified personnel who access the system or certified personnel who allow unauthorized personnel to access the system shall receive the following discipline;
1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review/Written Reprimand and Counseling
3rd Offense - Corrective Review/Suspension
4th Offense - Corrective Review/Termination

k. Inquiries - Inquiries are to be for Criminal Justice purposes only. There are to be no CURIOSITY inquires.

i. Personnel in violation of this policy shall receive the following discipline;
1st Offense - Corrective Review/Written Reprimand
2nd Offense - Corrective Review /Written Reprimand and Counseling
3rd Offense - Corrective Review/Suspension
4th Offense - Corrective Review/Termination

l. Dissemination of Information - All operators shall adhere to NCIC/LLETS policies and procedures as well as all state and federal laws regarding inquiries that are transacted via NCIC/LLETS or ICJIS. This includes but is not limited to criminal history information. All information obtained via these systems is to be disseminated only to authorized criminal justice's employees in the official performance of their duties within the criminal justice agency. Under no circumstances is any information received via these systems to be released to any member of the public or unauthorized persons. Inquiries from the public and or individuals other than authorized criminal justice personnel may be directed to the appropriate office/section within the Department of Public Safety.

i. Personnel found in violation of this policy shall receive the following discipline;
1st Offense - Corrective Review/Suspension
2nd Offense - Corrective Review/Termination

m. Individual Operator Log Required

All inquiries into Thinkstream (NCIC/LLETS) should be recorded on an office Greater Lafourche Port Commission log form provided to you and turned in on your last working day of the month.

i. Personnel in violation of this policy shall receive the following discipline;
   1st Offense - Corrective Review/Written Reprimand
   2nd Offense - Corrective Review /Written Reprimand and Counseling
   3rd Offense - Corrective Review/Suspension
   4th Offense - Corrective Review/Termination

n. HIT Confirmations - When an inquiry on an individual or property yields a valid positive response (hit), the printout showing the inquire message should be retained for use in documenting probable cause for detention of the missing person, arrest of a wanted person, or seizure of property. The terminal operator shall document precisely how, when and to whom the information was given, initial and date this notation and forward to Investigations and Records for retention in the case file. This establishes Chain of Evidence. The printout should be retained for as long as remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. Once the case has been resolved and there is no longer a possibility of a lawsuit the printout must be destroyed by tearing or shredding to prevent unauthorized access in accordance with the retention schedule of the Greater Lafourche Port Commission.

i. Failure to comply with this policy shall result in the following;
   1st Offense - Corrective Review/Written Reprimand
   2nd Offense - Corrective Review /Written Reprimand and Counseling
   3rd Offense - Corrective Review/Suspension
   4th Offense – Corrective Review/Termination

o. When an employee separates employment with the Greater Lafourche Port Commission, Wide Area Network, ICJJS, and NCIC Query privileges are deleted. The State of Louisiana will be notified to remove the employees name from NCIC user authorization.