GREENVILLE COUNTY
SHERIFF'S OFFICE

GO - 234

GENERAL ORDERS

COMPUTER SYSTEMS, ELECTRONIC MEDIA AND OTHER ELECTRONIC SYSTEMS

PURPOSE:

Efficient, effective and secure communication is essential to the operation of the Sheriff's Office and the County of Greenville. The purpose of this policy is to establish and provide guidelines in the proper use of electronic equipment, systems, tools and resources provided to employees by the County of Greenville, the Sheriff's Office, SLED, NCIC, CJICS or other sub-systems and approved service providers.

POLICY:

Resources available to employees from all computer and electronic informational systems or electronic media are to be used to further the goals and objectives of the Sheriff's Office and the County of Greenville by providing an effective method to:

- Communicate.
- Perform research.
- Obtain information while performing law enforcement related tasks.

Employees are expected to use good judgment while using any and all computer related resources and electronic media. Employees are to abide by the following:

- All software licensing agreements and restrictions.
- User agreements between the employee and this Office or the employee and other departments within the County of Greenville.
- Requirements set forth by SLED, NCIC and CJICS.
- All applicable security requirements set forth by this Office, the County of Greenville, State and Federal Agencies, or other sub-systems and approved service providers.

PRIVACY:

Electronic media, specifically the Internet and e-mail, is not a secure communication network, and others can potentially read personal or privileged information via these media.

Employees have no expectation of privacy:

1. In sending or receiving electronic messages and information on the Internet or the MDT System.
2. With computer workstations, equipment, hardware and software owned by this Office or the County of Greenville.

NOTE - *This Office reserves the right to monitor, inspect and audit all electronic messages and information received, sent or distributed through any computer system owned by this Office and the County of Greenville, or accessed by our computer system.*

INTERNET:

The Internet is a legitimate law enforcement resource and investigative tool. All personnel are to adhere to the following when accessing the Internet:

1. Use of the Internet is for legitimate law enforcement purposes only.
2. The Internet is not to be used in any manner deemed inappropriate.
3. Accessing offensive and inappropriate websites is prohibited unless a legitimate law enforcement need exists and only with prior supervisory notification and subsequent approval.
4. Internet game playing is prohibited.

E-MAIL AND MESSAGING SYSTEMS:

E-mail and messaging systems are valuable tools that can enhance the effectiveness and efficiency of the Sheriff's Office. Employees are to adhere to the following guidelines for e-mail / messaging use:

- The e-mail and messaging system is to be used for business purposes only.
- There is no expectation of privacy between e-mail or messaging system users.
- The e-mail and messaging system is subject to routine monitoring.
- Use of inappropriate or offensive language is prohibited.
- All e-mail and messaging system text is subject to public review via the Freedom of Information Act.

The Office of Professional Standards will perform a documented quarterly review of MDT messages to ensure the proper use of the system.

MOBILE DATA TERMINALS:

MDT's are to be operated in accordance with procedures outlined in the Premier MDT Manual.

NCIC USAGE:

The Greenville County Sheriff's Office is responsible for security of SLED/CJICS/FBI files within our agency. Guidelines are in place to enhance security of the use of these files. Each certified operator is responsible for insuring this policy is adhered to at all times through the use of SLED functions by interface systems, Mobile Data Terminals, KMS software and the SLED terminals which have a direct line to SLED.

Data stored in NCIC is documented criminal justice information, and must be protected to ensure correct, legal, and efficient dissemination and use.
The individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the data. The stored data in NCIC is sensitive and should be treated accordingly. An unauthorized request or receipt of NCIC material could result in criminal proceedings or interdepartmental disciplinary action of any infraction of the misuse of the system. This policy includes correct documentation for entry purposes as well as inquiries.

All NCIC/SLED/CJICS/DMV systems are to be used for law enforcement purposes only and should not be disseminated to the public.

GREENVILLE COUNTY WIDE AREA NETWORK (WAN) – Due to SLED/NCIC requirements, employees with wireless access to the WAN must notify the Office of E911 as soon as possible in the event of a loss or theft of a wireless device used to access the network.

These devices include, but are not limited to:

- Mobile Data Terminal
- Wireless laptop accessing SLED/NCIC
- Vehicular Radio Model
- Any 802.11 type PC wireless card

Once notified of a loss or theft of a device, E911 will accomplish the following to reduce the chance of access to the network:

1. Remove the MDT device ID from the PMDC (SCART) server.
2. Remove the VRM device ID from the Radio Net Controller (RNC).
3. Remove the 802.11 device ID from the Wireless Access Points (WAPs).

CENTRAL COMPUTER SYSTEMS:

COMPUTER AIDED DISPATCH (CAD) – The Office of E-911 is responsible for maintaining the CAD System.

CAD Data Backup and Storage - All CAD data is stored on the Non-Stop Server, also known as the "Tandem," for a period of two-years. A complete system backup and an Event/Audit backup are performed monthly on the Tandem. While performing this backup, the CAD System users are not affected with down-time.

The archival tape that is used to store this information will be kept in an off-site location until such time that another full backup is completed or it is needed for retrieval.

Data is also transferred to the UDT-DSS Server into an SQL Database, "IDT4." The UDT4 database is backed-up daily. This information is maintained on the UDT-DSS server indefinitely. There are six archival tapes and they are rotated every 2-days. These tapes are also kept at an off-site location.

Note- During upgrades to the Operating System or the CAD system, a full backup is performed before the upgrade is started.

CAD Access Security / Password Audits – CAD is equipped with an automated security system that authenticates every user by Employee Number and Password. A log on the Tandem authenticates users and records invalid sign-on attempts. As needed, Personnel Orders are cut to document an employee's resignation or termination. This order is sent to the Director of Communications who removes employees from the CAD System. As a back-up to Personnel Orders, each month the Administrative Services Division forwards a listing of employee terminations and resignations to the Director of Communications and the Office of E-911 to ensure the timely removal of former employees from the CAD System.

Records Management System (RMS) – The Information Systems Department is responsible for maintaining the RMS.

RMS Data Backup and Storage – Incremental and full back-ups of network and server files are conducted on a prescribed daily/weekly/monthly schedule. Backup media is transported to a secure off-site facility each day. Backup media is recycled as appropriate and secure destruction services are utilized for non-recyclable media.

RMS Access Security / Password Audits – The iSeries/AS-400 requires a user ID and Password to be entered and validated before a user has access to any application. Once a user is authenticated by the iSeries/AS-400 operating system, the user will have specific menu option access. An application security table is used to determine not only which applications and menu options a user ID has access to, but also what level of access within that application. Repeated invalid user attempts will lock a user's account and only Information Systems can re-enable the account. The Information Systems' Security Officer monitors reports daily for any suspicious logon activity. Employee resignations/terminations are forwarded to Information Systems via Human Resources for removal from RMS access.

As a back-up to Human Resources, each month the Administrative Services Division forwards a listing of employee terminations and resignations to E911 personnel and Information Systems to ensure the timely removal of former employees from the CAD System.

UNAUTHORIZED USE OF COMPUTER, ELECTRONIC, AND INFORMATION SYSTEMS:

Violations include, but are not limited to, the following:

- Using any computer, computer system or network facility without proper authorization.
- Assisting in, encouraging, or concealing from this Office or other authorities any unauthorized use, or attempted unauthorized use, of any computer, computer system or network facility.
- Knowingly endangering the security of any computer, computer system or network facility or willfully interfering with others authorized for usage of these systems.
- Giving away or sharing any password assigned to them to access any computer, computer system or network facility without proper authorization.
- Reading, altering, or deleting any other person's computer files or electronic mail without specific authorization.
- Downloading or introducing unauthorized programs or files.
- Manipulating or altering current software on agency owned mobile or desktop computer.
- Transmitting any material or messages in violation of Federal, State, local law or County policy, including sexually, racially, or ethnically offensive comments, jokes, slurs, threats, harassment, slanders, or defamation.
- Accessing or distributing obscene or suggestive images or offensive graphical images.
- Distributing sensitive or confidential information.
- Distributing unauthorized broadcast messages or solicitations.
- Using County provided electronic media to accomplish personal gain or to manage a business.
- Distributing copyrighted materials not owned by the County, including software, photographs, or any other media.
- Downloading copyrighted information or software.
- Developing or distributing programs designed to infiltrate computer systems internally or externally.
- Accessing or downloading any resource for which there is a fee without prior, appropriate approval.
- Attempting to access any system an employee is not authorized to access (hacking).
- Listening to voice mail or reading electronic mail of another employee without prior, written approval of the Sheriff.
- Endorsing political activities.
- Unauthorized modification or destruction of system data.

- Negligent loss of computer system capability.
- Negligent loss by theft of any computer system media including: chip ROM memory, optical or magnetic storage medium, hard-copy printout, and similar computer related material or mechanisms.

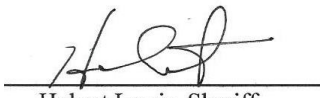
NOTE – The Sheriff, Chief Deputy and Majors are the only persons who may grant permission for installation of any additional software or programs to any county owned computer.

Only authorized computer equipment is to be connected to the computer network.

DISCIPLINARY ACTION:

Violations of this policy will result in counseling or disciplinary action appropriate to the violation. Disciplinary action may include one or more of the following:

- Written Warning.
- Written reprimand.
- Suspension from duty without pay.
- Demotion, if applicable.
- Termination of employment.
- Criminal prosecution.



Hobart Lewis, Sheriff