SUBJECT: COMPUTER SERVICES

TELEPHONE COMMUNICATIONS AND AUTOMATED DATA COMMUNICATIONS

A. The Chief Information Officer of the Information Technology Division (IT) of the Department of Justice will direct these communication functions. This includes, but is not limited to, providing the telecommunications network and data processing systems necessary to support voice and data needs throughout the Bureau. It also includes maintenance and operation of the law enforcement telecommunications network.

B. Requests for voice or data service or terminal connections will be coordinated between the appropriate Assistant Director and the IT Chief Information Officer.

C. Communications equipment such as csu/dsu's, routers, and hubs shall not be altered, relocated, or modified except by IT personnel or at their direction.

D. For Network Security purposes, no PC or Laptop is allowed to have a modem installed or be attached to a modem while connected to the network.

SBI INFORMATION SYSTEMS

The SBI operates its information systems within a client server environment consisting of various hardware platforms. These systems must remain secure and inter-operable. Therefore, development of user applications is the responsibility of the IT Division. IT support of these applications is dependent on the following procedures:

A. User Applications (Software Development)

New Applications

1. Requests for applications should be submitted in writing to the Special Agent in Charge or Supervisor who will forward, with a recommendation, to the appropriate Assistant Director.

2. When approved by the Assistant Director, the request should be made by using the SDLC Service Request Form and forwarded to IT. The Service request form may be downloaded from: **http://internal.jus.state.nc.us/it/SDLC/forms/request.wpd** (*revised 07/11/03*)

3. IT will evaluate the request and respond regarding development

possibilities or options.

Existing Applications

4. Requests for enhancements should be discussed with the appropriate IT support personnel. A Change Request Form should be completed. The Change request form may be downloaded from: **http://internal.jus.state.nc.us/it/SDLC/forms/change.wpd** (*revised 07/11/03*)

5. After discussion with IT personnel the request should be routed either through the Special Agent in Charge or Supervisor or appropriate Assistant Director for approval. The form will then be forwarded to the IT Applications Development Manager.

6. IT will evaluate the request and respond regarding development possibilities or options.

B. Applications Platforms (Operating Environment and Hardware)

1. Developed computer applications will reside on various hardware platforms located throughout the SBI and IT.

2. The installation and maintenance of these operating environments is the responsibility of the IT Division.

3. Only IT personnel are authorized to alter the operating environment of these platforms. Other employees may respond to directions from IT personnel.

4. "Alter" is defined to include relocation of hardware, software configuration changes, parameter changes, and anything else that would change the environment.

MICRO COMPUTING

A. Personal Computer Software Statement

1. The State Bureau of Investigation licenses the use of its personal computer software from a variety of outside companies. The SBI does not own this software or its related documentation and, unless

authorized by the software developer or publisher, does not have the right to reproduce it.

2. With regard to use on local area networks or on multiple machines, SBI employees shall use the software only in accordance with the license agreement.

3. SBI employees learning of any misuse of software or related documentation within the organization shall notify their immediate supervisor.

4. Before use of any PC software, SBI employees must become familiar with its license agreement.

5. The SBI does not require, request or condone unauthorized use of computer software by its employees. According to the U.S. Copyright Law known as the Computer Software Copyright Act, Section 117, Title 17, United States Code, illegal reproduction of software can be subject to civil damages of $50,000 or more, and criminal penalties including fines and imprisonment.

6. SBI employees making, acquiring or using unauthorized copies of computer software will be disciplined in accordance with policies and procedures established by the Office of State Personnel.

7. SBI employees must not install personal copies of licensed software on Bureau owned personal computers. Any software loaded on a state owned PC must be properly licensed by the agency.

8. SBI employees must not use State owned personal computers for any personal work or business.

9. The operating environment for stationary computer equipment shall not be altered, relocated, or modified except by IT personnel or at their direction.

B. Implementation of Personal Computer Software Statement

1. SBI employees have the responsibility for knowing the Personal Computer software procedure.

SUBJECT: COMPUTER SERVICES

2. All software residing on networked computers will be accounted for by the DOJ IT Division using an automated inventory tool called Asset Insight, furnished by the State Information Resource Management Division. Software inventory on Non-networked computers and Laptops must be collected via a semi-automated process for inclusion in the Asset Insight repository. IT Division will schedule a time each year for these machines to brought in for inventory purposes.

3. Employees will be given at least thirty days advance notice of the inventory process to schedule delivery of the machines.

4. Only properly licensed software will be allowed to be installed or reside on SBI personal computers.

5. Use of properly licensed software will be confined to the ones that have been defined as supported by the IT Division PC support personnel. Use of any other software, including public domain or shareware products, will be reviewed for compatibility and possible acceptance for support.

6. IT technical support will be confined to software products defined as supported by the IT Division PC support personnel. Use of any other software is discouraged and such software products will not be supported.

7. SBI employees will be made aware of the differences in Public Domain and Shareware software products. A copy of definitions of Public Domain and Shareware will be made available to employees as appropriate.

8. The IT Division will maintain a master inventory of all installed or licensed software and hardware assigned to Bureau personnel. The master inventory will be maintained in an automated system file located at DOJ IT. A copy of the file will also be maintained in state IRM master Asset Insight database. Each section will be provided a copy of their inventory file upon request.

9. Public domain utility programs which facilitate common PC operations may be used as long as they are placed together in a separate subdirectory.

10. Any public domain or shareware software used on any SBI machine must be checked by the IT Division PC support group for Virus contamination prior to installation.

11. Original program diskettes will be retained. Original diskettes should be secured for audit purposes. Individual employees will be responsible for the safekeeping of these diskettes.

12. A review of the PC Software Policy will be made a part of the New Employee Orientation.

C. SBI Statement for Home Use of WordPerfect Product

1. The State Bureau of Investigation (SBI) licenses the use of the WordPerfect product and is not the owner of this software.

2. Distribution of the WordPerfect product to a SBI employee complies with the product provision stated in its Software Licensing Agreement which states the following:

"You are authorized to use a copy of the Software on a home or portable computer, as long as the extra copy is never Loaded at the same time the Software is Loaded on the primary computer on which you use the Software."

3. The employee receiving authorization to use the WordPerfect product at home must clearly understand and abide by the above stated provision. Any misuse or noncompliance will cause the SBI to take disciplinary action in accordance with policies and procedures established by the Office of State Personnel.

4. The employee must furnish personally owned diskettes for the purpose of obtaining a copy of the product for home use.

5. Upon termination of employment, the employee must return the product to the SBI and simultaneously eliminate from the personal computer and personal diskettes, all related items which fall under the agreement.

6. By signing this agreement, the employee agrees to all statements

SUBJECT: COMPUTER SERVICES

mentioned above. A copy of this agreement will be maintained by the section supervisor. Additional records will be maintained in the IT Division's computerized Software Inventory system.

Employee Name: _____

Employee Signature: _____

Original License Loaded On: _____

Date Received: __/__/__ **Date Returned**: __/__/__

ELECTRONIC MAIL (E-MAIL)

All routine communications to and from SBI offices should be transmitted via E-Mail rather than through a switched message.

ELECTRONIC-MAIL (E-MAIL) SECURITY

A. The SBI reserves the right to review all electronic records.

B. The SBI prohibits employees from reading other employees' E-Mail, except in situations that require the access for legitimate government purposes. Attempts should be made to obtain the originator's consent.

C. The user should not use an obvious password, such as his/her name.

D. The user should always know to whom the E-Mail message is being sent. Addresses should be double-checked to avoid inadvertent, potentially embarrassing broadcasts.

E. The user should not send highly sensitive, confidential, or potentially embarrassing messages. Inflammatory messages should be avoided.

F. The user should exit E-Mail when leaving his workstation or use a password-protection screen saver.

SELF-MAINTENANCE OF DESKTOP COMPUTERS AND ATTACHED PRINTERS

SUBJECT: COMPUTER SERVICES

Office Desktop Personal Computers shall no longer be covered by vendor maintenance contract services beyond the warranty period. All such standard equipment on the IT Division's Computer Equipment Inventory shall be "self-maintained" after warranty expiration. Problem reporting shall be made through the PC/LAN Support Group of the IT Division's. Coordination of warranty service calls or swapping failed equipment with a workable replacement shall be determined by the IT Division.

IT'S RESPONSIBILITY FOR REPLACEMENT OF FAILED COMPONENTS

A. IT Division shall maintain a stock of equipment for replacing failed components.

B. Problem isolation shall be made between the user and IT technical staff.

C. Failed equipment shall be replaced with a minimum configuration. This replacement may be equipment other than the original equipment.

D. Replacement of the component shall be shipped or delivered by UPS, Federal Express, or an SBI employee.

E. The defective component shall be returned to the IT Division by UPS or a SBI employee.

F. To determine the cost of repair, the IT Division shall have an evaluation made of the defective equipment by a repair center.

G. Upon evaluation, the IT Division shall determine if the defective component should be repaired or surplused.

USER'S RESPONSIBILITY FOR FAILED COMPONENTS

A. The PC/LAN Support Group shall be contacted by telephone when problems occur with the desktop personal computers or printers.

B. The user shall receive a contact number and an attempt will be made to isolate and resolve the problem.

C. If not immediately corrected, the users problem shall be referred to the appropriate support group. If no one is available immediately, the user shall

expect a return call as soon as possible.

D. The user may be instructed to perform some minor checks to identify the exact problem.

E. In certain circumstances, the user shall be asked to try another monitor or keyboard to isolate the malfunction.

HARDWARE COVERED UNDER THE SELF-MAINTENANCE PROGRAM

All Office Desktop Computers, Monitors, 101/102 Keyboards, Mouse, Laser Printers and Dot Matrix Printers are covered under the self-maintenance program.

HARDWARE NOT COVERED UNDER THE SELF-MAINTENANCE PROGRAM

A. Computer Equipment Under Maintenance Contract: Critical sites requiring 24 hour availability or speciality computer equipment such as computer mainframes, telecommunications, UNIX servers, imaging technology and related printing devices shall be listed and bids submitted in order to receive vendor maintenance contracts. Assistant Directors shall be responsible for contracting service where needed..

B. Portable Equipment and Related Peripherals: After the initial warranty service contract expires, maintenance must be renewed either through the vendor or an authorized service center.

C. Specialized Equipment: Computerized laboratory hardware, special investigative equipment, and crime scene equipment shall not be covered by the new self-maintenance plan. It is the responsibility of the Special Agent in Charge, Supervisor or designee to monitor and extend maintenance coverage.

USE OF THE NORTH CAROLINA INTEGRATED INFORMATION NETWORK AND THE INTERNET
(REFER to DOJ Internet Policy: http://internal.jus.state.nc.us/it/policy/internet-policy.pdf
(*revised 07/11/03*)

A. Definitions

SUBJECT: COMPUTER SERVICES

1. E-Mail: Electronic Mail - The capability to compose, address, and send messages electronically.

2. NCIIN: North Carolina Integrated Information Network - refers to a web of interoperable networks, within the state, that transmits data, text, images, voice, and video.

3. World Wide Web: The integrated world wide network of computers based on the hypertext transfer protocol (HTTP), and Transmission Control Protocol/Internet Protocol (TCP/IP), commonly used to bring information to computer users via a client browser program.

4. Information processing resources: Electronic computing and communications hardware, software, networks, and information.

B. Use of NCIIN and the Internet

1. While in performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, public employees are expected to use the North Carolina Integrated Information Network (NCIIN) and the Internet responsibly and professionally.

2. Public employees shall make no intentional use of these services in an illegal, malicious, or obscene manner.

3. Public employees may make reasonable personal use of publicly owned or provided NCIIN or Internet resources as long as:

   a. The direct measurable cost to the public is none or is negligible.

   b. There is no negative impact on employee performance of public duties.

   c. The policy is applied equitably among all employees of the agency.

   d. Employees shall reimburse the agency if costs are incurred, provided that costs may be incurred only in critical situations.

4. When sending or forwarding E-Mail over the NCIIN or the Internet, public employees shall identify themselves clearly and accurately. Anonymous

or pseudonymous posting is expressly forbidden. (Any exception to this procedure for Agents working in an undercover capacity must be approved by the Special Agent in Charge, Supervisor, or the Assistant Director of the affected District/Section/Unit. Where possible all undercover investigations through the Internet should be conducted from an undercover Internet account and not from an identifiable state computer.)

5. Public employees have a responsibility to make sure that all public information disseminated via the NCIIN and the Internet is accurate. Employees shall provide in association with such information its source and the date at which it was current and an electronic mail address allowing the recipient to contact the public staffs responsible for making the information available in its current form.

6. All files downloaded from a source external to the NCIIN must be scanned for viruses. This includes files obtained as E-Mail attachments and by any other file transfer mechanism. It is the responsibility of public employees to prevent the introduction or propagation of viruses.

7. The Internet provides easy access to software distributed by companies on a trial basis. This free access does not indicate that the software is free or that it may be distributed freely. All applicable software copyright and licensing laws must be followed.

8. Using Internet Webcasts for personal reasons uses valuable network bandwith and may interfere with normal business data flow. DOJ policy prohibits the use of computers for this purpose. Examples include: Media Players accessing streaming audio and video broadcasts.