

**OFFICE OF INVESTIGATIVE SERVICES
POLICY & PROCEDURE #410**

COMPUTER POLICY

USE OF NON-DEPARTMENT OWNED COMPUTER HARDWARE OR SOFTWARE:

- The use of non-State of Georgia (hereafter referred to as Department) owned computers is authorized for official business provided no state files are retained on the hard drive or personal floppy discs.
- Use of non-Department owned software on a personal computer for work purposes is authorized provided that the user can demonstrate, through appropriate documentation, that the software was legally purchased and is being used in a manner consistent with the software license, user agreement, etc.
- Employees using their personal computers for work related purposes will not be compensated for any damages resulting out of such use. Any use of a personal computer is at the risk of the individual.

PASSWORDS; ACCESS RIGHTS; COMPUTER SECURITY:

Employees are responsible for maintaining the security of Department computers and systems due to the sensitivity of information that may be contained therein. Although data, information, files, email and other electronic communications are subject to review by authorized members of the Department, employees are not authorized to access information beyond the scope of their duties and authorized uses.

- Employees will not share their password with others, or cause their password information to be distributed to others for any reason.
- Password or computer/service access information will not be written or left in a manner that would allow others to access Department computer or systems.
- Employees are not authorized to access, read, alter, or modify email messages under another's access rights. Employees are not authorized to enter another employee's email without prior authorization from the Director.
- Whenever an employee is leaving a workstation, they are responsible for security of any software programs, network service access, email services, or other programs to prevent unauthorized access by others.

ELECTRONIC MAIL POLICY STATEMENT:

The Department maintains as part of its technology platform an electronic mail system, commonly known as GroupWise or Go Mail. This system is provided to assist in the conduct of business within the Department. All computers and the data stored on them are and remain at all times the property of the Department. As such, all electronic-mail messages composed, sent and received are and remain the property of the Department.

The Department reserves the right to retrieve and read any message composed, sent or received. Please note that even when a message is erased, it is still possible to recreate the message; therefore, ultimate privacy of messages cannot be guaranteed to anyone.

Messages should be limited to conducting Department business. Electronic mail may not be used to conduct personal business.

While electronic mail may accommodate the use of passwords for security, the reliability of such for maintaining confidentiality cannot be guaranteed. You must assume that someone other than the intended or designated recipient may read any and all messages.

COMPUTER POLICY (continued)

Except as set forth above, all messages sent via electronic mail are considered to be confidential and such are to be read only by the addressed recipient or at the direction of the addressed recipient. The Director must approve any exception to this policy.

Employees learning of any misuse of the electronic-mail system or violations of this policy shall notify their immediate supervisor.

E-mail messages may not contain content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but not be limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that would reasonably be considered offensive.

POLICY CONSIDERATIONS:

The OIS Network Administrative Team Leader (OIS NATL) is responsible for the coordination of all computer and network services to include hardware and software. All computer data, files, electronic communications, whether Department related or private, are considered property of the Department and shall remain at all times. Authorized Department personnel may access, review, audit and/or monitor computer and computer systems use of all employees at any time without prior notice.

SOFTWARE INSTALLATION/INVENTORY:

Maintaining an accurate inventory of all software products located on individual Department computers/systems will ensure proper operations. Inventories will ensure that properly updated software for Department use is maintained.

- Employees are not authorized to remove, alter, or otherwise modify any software loaded on their Department computers unless approved by OIS NATL. Software programs are to be upgraded by authorized personnel only. The supervisor will ensure a software inventory is conducted of all Department computers annually. Inventory will include the name, version, manufacturer and serial number of the software programs and where the software resides.
- All requests for the purchase of new software, or upgrades to existing software must be approved by DHR IT.
- Software located on a specific computer that will no longer be utilized will be removed by authorized personnel only. All documentation, CD's or discs will be turned over to OIS NATL upon removal from the computer.

COMPUTER/NETWORK SYSTEMS PROTECTION; VIRUSES:

Computer viruses are a threat to the proper operation of Department computers and systems. Computer viruses can only be introduced by file transfers, copying or email attachments. To protect Department computers and systems, employees are not authorized to introduce foreign programs, files or email attachments without permission of the OIS NATL.

- Software, floppy discs, or emails from unknown sources will not be introduced to Department computers or systems.

COMPUTER POLICY (continued)

COMPUTER AND NETWORK SERVICE SETTINGS

To ensure the proper operation of Department computers and network services, employees are not authorized to change settings, alter programs, etc. that will modify, alter or otherwise change the computer or services operations. Examples include, but not limited to; changing user settings beyond approved ranges, modifying autoexec.bat files, command.sys files, etc. All employees should receive authorization from OIS NATL prior to making any changes in the computer or network service operations systems.

UNAUTHORIZED COMPUTER USE

Computers and systems provided by the Department are for business purposes only. Employees must be aware of unauthorized uses of Department computer systems will subject them to disciplinary action, up to and including dismissal.

- Computers and/or systems provided by the Department will not be utilized for purposes other than Department business.
- Employees are not authorized to use Department provided Internet services for the viewing of web sites containing material, such as:
 - Adult entertainment related
 - Information for committing illegal offenses, (except as authorized for investigations),
 - Material that could reasonably be considered offensive to others, whether accessed privately or in the open.
 - Access an electronic service to express opinions of a personal or political nature.
 - Conduct or activity that is derogatory, discriminatory, or offensive to any race, gender, ethnicity, religious or age group.
 - Participate in a service that promotes or facilitates illegal or unethical activity.
- Employees will not utilize computers or systems to transfer criminal history information unless authorized by GCIC rules & regulations.
- Employees will not copy, transfer, alter, delete or otherwise access any data, files, programs, without proper authorization.
- Employees will not subvert or bypass security procedures installed by a computerized electronic service provider.
- Employees will not access or attempt to access a restricted service without approval from a service provider.
- Employees will not violate any applicable local, state or federal statutes.
- Use any computer or system that is inconsistent with the goals and objectives of the Department or would constitute a violation of Department procedures, policies or practices.

O.C.G.A. 16-9-94. Venue.

Statue text

For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

1. In the county of the principal place of business in this state of the owner of a computer, computer network, or any part thereof;
2. In any county in which any person alleged to have violated any provision of this article had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation;

COMPUTER POLICY (continued)

3. In any county in which any act was performed in furtherance of any transaction which violated this article; and
4. In any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

History

(Code 1981, § 16-9-94, enacted by Ga. L. 1991, p. 1045, § 1; Ga. L. 1992, p. 6, § 16.)

Annotations

Cross-references. – Venue generally, Ga. Const. 1983, Art. VI, Sec. II, Para. VI and § 17-2-2.