Georgia Department of Public Safety
Policy Manual

SUBJECT **COMPUTER SECURITY AND CRIMES**	POLICY NUMBER **14.02**
DISTRIBUTION **ALL EMPLOYEES**	REVISED DATE **8/3/2018**
	POLICY REVIEWED **8/3/2018**

14.02.1 Purpose

All Department employees should be aware of the various areas that constitute illegal computer activity. Persons found to be in violation of this policy are subject to criminal charges under the current law and disciplinary actions by the department.

14.02.2 Policy

It shall be the policy of the Georgia Department of Public Safety to provide competent protection for all computer equipment and software against any type of criminal or illegal activity. This protection will cover all computer related activities. The policy encompasses computer theft, trespassing, invasion of privacy, forgery and password disclosure.

Penalties invoked under O.C.G.A. §§16-9-90, 16-9-91, 16-9-92 and 16-9-93 for these illegal activities are a fine of not more than fifty thousand dollars and/or imprisonment of not more than fifteen years.

14.02.3 Definition of Terms

A. Computer - an electronic, magnetic, optical, electromechanical, or any other high speed data processing device or system performing computer operations with or on data and includes any data storage facility, printing, or communication facility directly related to or operating in conjunction with these devices.

B. Computer Network - an established number of related computers and/or terminal devices connected together and any communications facilities with the function of transmitting or receiving data to or from these computers or devices through communication facilities.

C. Computer Program - one or more statements or instructions composed and structured in a form acceptable to a computer. The statements or instructions when executed by a computer in actual or modified form will cause the computer to perform one or more computer operations. This shall include all associated procedures and documentation whether or not they are in human readable form.

D. Data - any representation of information, intelligence, or data in any fixed medium including documentation, computer printouts, and magnetic storage media stored in a computer or transmission by a computer network.

E. Financial Instrument - any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debt form, transaction authorizing mechanism, or marketable security or the computer representation thereof.

F. Property - all computers, printers, modems, transmitting devices, computer programs, data, financial instruments, services, or any interrelating devices or documents.

G. Services - any computer time or data processing function.

14.02.4 Provisions

A. Georgia law and Georgia Department of Public Safety policy prohibit all employees, consultants and contractors of the DPS from committing any of the following:

1. Computer Theft

    a. Using a computer or computer network without the authorization of the immediate supervisor.

    b. Physically removing any property such as computers, printers, modems, or any other related hardware without the permission of the supervisor.

    c. Displacing or altering any computer software such as programs, services, data networks, or financial instruments.

    d. Removing and/or copying licensed software from a Departmental facility for personal use.

2. Computer Trespassing

    a. Using a computer or computer network with the knowledge that the use is without authority and with the intent of the following:

        1) Deleting or in any way removing, either temporarily or permanently, any program or data from a computer or computer network;

        2) Obstructing, interrupting, or in any other way interfering with the use of a computer program, data, or network; and/or

        3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program.

3. Computer Invasion of Privacy

    Unauthorized use of a computer or computer network to examine or obtain any data regarding employment, medical, salary, credit, financial, or any other personal data relating to an individual.

4. Computer Forgery

    Creating, altering, or deleting any data contained in any computer or computer network without authorization from a supervisor.

5. Computer Password Disclosure

Disclosure of a number, code, password or by other means accessing a computer or computer network knowing that such disclosure is without authority.

B. The Technology Director, who is responsible for computer security will at least annually conduct an audit for the verification of passwords, access codes and any access violations.

C. To prevent against the loss of electronic information, the Technology Director shall ensure that backup copies of all network drives are made each business day. The backup copies shall be stored for at least 60 days.