Apex Police Department
General Order

Title	Order Number
Computer/Software Security	403-22
Effective Date: February 7, 2022	**Amends:** General Order 403-15
CALEA Standard: 11.4.4, 41.3.7, 82.1.6	**Rescinds:**
Reference: Town of Apex Information Technology Policy, Criminal Justice Law Enforcement Automated Data Services (CJLEADS), Access Policy Division of Criminal Information (DCI) Policies and Regulations GO 401 – Records Administration GO 1204 – DCI Operations and Security	**Pages:** 5
Forms:	

Computer/Software Security

Purpose

The purpose of this directive is to establish procedures for the secure introduction of computer software and external data into a computer controlled by the Apex Police Department.

Policy

It is the policy of the Apex Police Department to establish procedures in compliance with the Town of Apex Administrative Policy and Procedure 300 – *Policy on Information Technology* for the installation of external data or software on computers issued or supplied by the Apex Police Department.

Definitions

Computer – A programmable electronic device that can store, retrieve, and process data. These devices include but are not limited to commonly known computer forms such as a workstations, desktops, laptops, tablets, and mobile computers.

Data – Anything that can be stored electronically by a computer.

Hard Drive – The mechanism that reads and writes data.

Software – A collection of computer instructions or data. The software can be on media such as a DVD, CD, USB drive, and external hard drive.

Procedure

1. Town of Apex (TOA) IT is designated as the custodian over all computers and software for the department and will maintain accurate inventories of all computers and computer-related equipment. In addition, the original software programs purchased by the department are to be maintained in a secure manner.

2. IT personnel must approve all software installed or accessed on department computers. The decision to approve and purchase new software will be based on issues of the need for the specific software, use, compatibility, cost, benefit, licensing, and other concerns. (41.3.7 (c)) (11.4.4)

3. The use or introduction of unauthorized computer software or external data not approved in department-controlled computer equipment or systems is strictly prohibited.

    - **NOTE:** The use of unauthorized computer software, programs, or external data could result in the introduction of viruses or other problems into the computer system. (41.3.7 (c)) (11.4.4)

4. Software will not be altered, manipulated, duplicated, or reproduced for use on other department computers, for personal use, or any other purpose without approval from TOA IT.

    - Computer software and programs will be copied only within the limits of the licensing agreement.
    - Illegal use of pirated software may subject the user/employee to both criminal and civil penalties. (41.3.7 (d))

5. Employees will maintain only police-related and approved software or external data on any hard drive that is connected to a department computer. Unauthorized data discovered on a department's computer hard drive may be deleted without prior notice to computer users. (41.3.7 (b)(c)) (11.4.4)

6. Network and Records Management System (RMS) passwords will be changed at least annually through an automated reminder. If the password is not changed within a set period, access will be automatically denied by the system. (82.1.6 (c)) (82.1.6 (d))

Data Security, Access, Storage (41.3.7 (b))

1. IT personnel are responsible for ensuring the security of all department data and systems.

2. All central records data will be stored in an approved RMS. (82.1.6 (b))

    - Access is limited to only those authorized as outlined in General Order 401 – *Records Administration* and any other applicable written directives.

3. The RMS main server is located in the police facility server room.

    - The RMS server is subject to a daily, automated backup. (82.1.6 (a))
    - The backup servers are located [redacted: This information has been redacted pursuant to N.C. General Statute 132 - Public Records.].
    - All RMS data is encrypted with access limited to approved Town IT staff.
        - All employees with access to police information must be pre-approved and are subject to a criminal history check as required by the North Carolina State Bureau of Investigation (SBI).

4. Users must first obtain an access code in order to access department-controlled computers. All access codes and passwords will be treated as confidential and will be restricted to the person to whom they have been assigned. (82.1.6 (c))

North Carolina/Other Computer and/or Data Systems (41.3.7 (b))

1. Criminal Justice Law Enforcement Automated Data Services (CJLEADS):
    - This system is governed by the North Carolina Office of the State Controller
    - Employee access and use will be in compliance with applicable rules, regulations, policies, and written directives related to this system

2. Division of Criminal Information (DCI):
    - This system is governed by the SBI
    - Employee access and use will be in compliance with applicable rules, regulations, policies, and written directives related to this system, including General Order 1204 – *Division of Criminal Information(DCI) Operations*

Termination of Employment/Suspension

1. Upon termination of employment for any reason (i.e., resignation, retirement, etc.), IT personnel and the Records Supervisor will:
    - Immediately disable access to all department computer systems
    - Notify all applicable agencies (i.e., NC AOC, SBI, etc.) that a person is no longer an employee of the department
    - Annually, as part of the annual audit, delete user access profiles from all systems

2. Upon suspension of employment for any reason, the Records Supervisor or his/her designee will:
    - Immediately disable access to all department computer systems until the suspension is lifted

Computer Users (41.3.7 (a))

1. The department seeks to facilitate computer usage among its employees while avoiding the pitfalls of unrestricted access.

2. Employees approved to use departmental computers will be required to read, acknowledge receipt of, and adhere to the TOA Administrative Policy and Procedure 300 – *Policy on Information Technology,* this General Order, and any other applicable written directive.

    - Employees will acknowledge receipt of these written directives during a TOA sponsored new employee orientation and/or during a department field training or civilian orientation program.
    - Employees who have not read and acknowledged receipt of the above-mentioned written directives are not authorized to use any computer equipment owned, used, or controlled by the department and/or the TOA.
    - Violation of the TOA Administrative Policy and Procedure 300 – *Policy on Information Technology*, this General Order, and any other applicable written directives can result in termination of user rights as well as disciplinary action.

Annual Updating and Audit (41.3.7 (c)(d)(e))(82.1.6 (d))

1. Annually, IT personnel will conduct a review of all computers and authorized users, as well as audit all passwords on agency systems.

    - IT personnel and the Records Supervisor will inactivate, remove, or cause to be removed users who are no longer employed by the department and will, if necessary, adjust access based upon current assignments.
    - The review will include verification that only approved software is installed on all department owned or controlled computers, systems, and hardware. (11.4.4)
    - The review will be completed and submitted to the Chief of Police no later than February 25th of the year following the period subject to the review.
        - The date may be extended with the written approval of the Chief of Police.

2. During the software update process, or at least annually, IT personnel will inspect each computer device to verify that no illegal or unauthorized computer software is being used. The results of the inspection will be included in the annual review. (11.4.4)

Text in “Green” denotes a significant change in policy

BY ORDER OF:

Jason P. Armstrong
Chief of Police