3.2.01 PURPOSE AND POLICY

The purpose of this directive is to establish responsibilities for the acquisition, budgeting, development, training, use and maintenance of the Department’s computer resources.

It is the policy of the Department to manage information technology efficiently and effectively in order to accomplish the Department’s mission. It is the policy of the Technology, Data and Analysis Division (TDAD) to provide guidance and assistance in the acquisition, installation, training and use of computer equipment and programs within the department. This includes budget preparation, computer supply management, and review of purchase requests for continuous oversight of the department’s computer activities.

3.2.02 DEFINITIONS

ACJIS - Alexandria Comprehensive Justice Information System. [82.3.6; 82.3.8]
AS/400 - IBM mid-range computer used for the records management and CAD systems. [81.2.4]
CAD - Computer Aided Dispatch.
CRIMES - the current vendor’s name for the records management software.
hardware - computer equipment. [82.3.1]
ITS – the City’s Information Technology Services.
ITSC - Information Technology Steering Committee; the City’s technology oversight committee. [82.1.3; 82.2.1]
LAN – local area network.
PRISM – (Police Reporting and Investigative Search Module) In-house query and reporting application.
RMS - records management system
software - computer programs.
software license – user’s agreement to operate computer programs.
upgrade - latest version of improved computer programs.
WAN – wide area network.
SRS Viewer – Geographic Information System application created by the City’s GIS Department to help users view and query crime, calls for service, arrests and field interviews geographically.

3.2.03 RESPONSIBILITIES

A. The TDAD commander will ensure the following tasks are accomplished.
   1. Annual report preparation;

   2. Annual TDAD budget preparation; [17.2.2]

   3. Supervision and training of TDAD staff;

   4. Develop and implement internal TDAD policies and procedures;

   5. Recommend approval or disapproval, or other actions relating to the procurement or development of computer applications, equipment, programs or supplies;

   6. Coordinate department automation plans, resources and policies with ITS, particularly the ITSC;

   7. Designation and training of systems automation representatives and backup personnel;

   8. Represent the Department at local, state and national criminal justice meetings, conferences, and seminars dealing with automation;

   9. Coordinate grants that impact the automated systems of the Department;

   10. Collaborate in the annual planning for future Department automation;

   11. Recommend automated equipment, software and training needed to meet Department accreditation standards;

   12. In coordination with ITS and in compliance with written city standards, develop and maintain Department standards for computer-related equipment, programs, supplies, and services;
13. Recommend modifications to ITS standards via the police chief, when appropriate, to more efficiently accomplish the department's mission;

14. Conduct periodic inspections of computer-related equipment and software, where and when necessary. Discovery of an unauthorized item may result in it being removed from the system. Notification of such discovery and removal shall be forwarded to the police chief. A copy of this notification will be given to the unit commander, who will then prepare a written response to the police chief;

15. TDAD personnel will continuously maintain and inventory the department’s computers and peripheral hardware;

16. Chair the Police Information Technology Committee (PITC). Personnel who want a project to be reviewed by the PITC must bring it forward to the Division Chief of TDAD for initial review.

B. Commanders will ensure that:
   1. Unit personnel are trained to operate computer systems under their responsibility, and substitutes are trained to operate systems when principal operators are absent;

   2. All equipment, software, publications, textbooks, magnetic tapes, disks, supplies and other computer items that are department property are properly maintained and accounted for and available for use by trained and authorized members of the department;

   3. Unit personnel follow the rules of all licensed computer programs and systems in use within their unit.

   4. Prepare a written response to the police chief, with a copy to the TDAD commander, when notified of an unauthorized computer-related item. (see section 3.2.03.A.14, above).

C. All personnel will:
   1. Care for and protect Department computers, equipment, software, and supplies.

   2. Obtain permission from the TDAD commander or designee prior to installation of any hardware or software.

   3. Implement significant alterations of computer systems only in coordination with TDAD staff. This includes but is not limited to the creation of LANs or installation of additional programs, drives or memory.
3.2.04 PROCUREMENT PROCEDURES

A. All Purchase Requests (APD-78) for computer equipment, software, training, supplies, services or related items, regardless of cost and whether budgeted or unbudgeted, will be routed through the TDAD commander in accordance with Police Directive 1.7, Fiscal Management.

B. No employee will commit the department to the receipt or exchange of computer services, purchases, training, computer related travel for training or demonstrations, maintenance, or product evaluations without first obtaining approval from the TDAD and Fiscal/Fleet Management commanders. Employees making or authorizing unapproved expenditures will be held accountable for their actions, and may be held financially responsible.

C. Emergency purchases requiring immediate delivery or repair due to unforeseen circumstances or to ensure public safety will be coordinated with the TDAD commander in compliance with guidelines contained in Police Directive 1.7, Fiscal Management.

D. TDAD personnel will advise commanders in the preparation of automated budget justifications. Commanders will ensure that requests for assistance are made in a timely manner to allow proper coordination prior to submission to Fiscal/Fleet Management.

E. TDAD will not be responsible for budgeting for any items under the purview of ITS. This includes but is not limited to, personal computer and network laser printer maintenance, LAN and WAN line/software and hardware costs, ACJIS equipment, line costs, mainframe processing, storage costs, mainframe programming and mainframe maintenance.

F. When appropriate, new software or system requests must be brought to the Police Information Technology Committee (PITC) for assistance and approval. See section 3.2.08 for information on projects, technologies and systems that qualify for the PITC.

3.2.05 RECEIPT OF COMPUTER-RELATED ITEMS

A. The TDAD commander will be notified upon receipt of all computer equipment, software programs, and commencement of computer services, regardless of the cost of such items. The original or a copy of all packing receipts will be immediately forwarded to the TDAD commander.
B. All registrations, licenses, and warranty cards and forms will be completed using the following information:
   Technology, Data and Analysis Commander
   Alexandria Police Department
   2003 Mill Road
   Alexandria, VA  22314
   Telephone: (703) 706-3975

   Under no circumstances will warranty or registration be made using individuals' names for products that are department property. In addition, all items to be used to purchase future upgrades, such as title pages, are to be forwarded to TDAD for storage and future upgrade use.

C. **Authorized software are those computer programs:**
   1. Purchased for use by ITS and APD from authorized funds or procured under any technology transfer agreement, Federal or State grants, or asset forfeiture funds;
   2. Procured by individuals using personal funds and licensed, registered, or authorized to be installed on a department computer. Proof of such permission will be personal possession of original disks, manuals, and licenses. Installation and use must comply with the manufacturer's license; and
   3. Equipment, procedures, texts, or publications provided to the department through the TDAD commander or the police chief.

D. When members of the department provide personal computer equipment for personal use with department software or equipment, it will be clearly labeled as such.

### 3.2.06 SYSTEMS BACK-UP AND SECURITY

A. The **TDAD Division Chief** will ensure that written guidelines exist for CAD/RMS system failure. These backup guidelines will be maintained in the Communications commander’s office and will consist of an emergency contact list of all TDAD personnel and APD employees trained in the operations of computer systems deemed operationally imperative by the police chief.

B. The **AS/400 system administrator** will:
   1. Ensure central computer systems are regularly backed up
      a. Critical AS/400 files are replicated to a redundant system at an offsite location.
      b. Daily backups are run on the redundant system.
      c. Weekly backups are run on the primary system.
      d. Any tapes that are discarded from the above system should be erased to ensure that data is not retrievable.

   2. Ensure security of computer records
      a. The regular disabling of passwords will take place:
         - During routine changing of passwords as a general security precaution, or
         - When a person has left the Department’s employment.

   [82.1.6]
b. Access codes, access violations and passwords are determined at the discretion of the system administrator.

c. The system administrator can set how often passwords expire. This is currently done at 160 days after the password was first set.

d. The system administrator can set the number of incorrect attempts that will be allowed before a login is disabled. This is currently set at 10 attempts. After that the system administrator must reset the user’s access to the system.

e. The system administrator or designee will conduct an audit of passwords, access codes and other security devices annually during January.

### 3.2.07 SOFTWARE DEVELOPMENT POLICY

A. Software developed under the following conditions give exclusive ownership rights to the department and the City:

1. Using departmental equipment, supplies or facilities; or

2. Developed during hours of employment; or

3. Incorporating or depending on Department information or data for development; or

4. Developed for departmental research or development.

B. **Employee written software:**

   1. Software written by department employees independent of the above which is brought into the Department and used to support the Department’s business gives the Department permanent right to use, but not ownership of the source code of the software.

   2. Employees engaging in private profit making by representing computer software or hardware manufacturers may not participate in the evaluation of that software or hardware products for use by this department while employed by this department. Employees may not use Department employment to indicate or imply that this department endorses the product(s).

### 3.2.08 POLICE INFORMATION TECHNOLOGY COMMITTEE (PITC)

1. The Police Information Technology Committee is comprised of 14 sworn and civilian police personnel of varying ranks and assignments and is chaired by the Division Chief of Technology, Data and Analysis. This group functions as a steering committee that presents new technology projects to the Chief for final approval.

2. The committee votes on new technology projects with the Division Chief of Technology, Data and Analysis having the deciding vote in the case of a tie.
3. Before voting, the committee will assess the following factors:
   a. If adequate staff time can be devoted to the project;
   b. Project timelines and delivery date;
   c. Funding for the project and staff member involvement (sworn and/or civilian);
   d. Automation of manual tasks;
   e. Ensure greater officer safety;
   f. Streamline current processes;
   g. Simplify routine administrative tasks.

4. To bring a project forward to the committee, a police employee must complete a Police IT Project Justification Statement (APD-0220). This document must be completed and presented to the Police IT Steering Committee for consideration.

5. The committee’s duties include reviewing proposed software/project descriptions on the APD-0220 and evaluating new and emerging technology the department wants to purchase and implement.

6. The committee will also determine who the Department project manager will be, and who will be needed to support the project on varying levels.

7. The Police Information Technology Project Committee is impaneled to review the following types of technology requests:
   a. Any software that will create data that will be extracted and analyzed by staff.
   b. Any software that will interface with our Records Management System (CRIMES), Computer Aided Dispatch (CAD), Field Reporting or MDB.
   c. Any software or system that will replace or enhance current system capabilities.
   d. Any system, application or software that will use or interact with wireless network capabilities.
   e. Any system, application or software that will require police Technical Support staff assistance.

8. Police staff must send these project descriptions (and any technology requests/proposals) to the Division Chief of Technology, Data and Analysis for discussion. These requests must fit into one of the categories listed above in order to be considered by the committee.

9. The committee meets once every two months, or as needed, to review and discuss project descriptions.

By Authority Of:

David P. Baker
Chief of Police