Anchorage Police Department Regulations and Procedures Manual	Operational Procedures 2.02.000-005	
Policy and Procedure Title Department Communications Computer Use and Procedure Policy	**Effective Date** 8/5/2009	Page 1of 8
Replaces Prior Policy: 4/22/2008	**Approved by:** Chief Rob Heun	

This policy is the internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.

2.02.000 Department Communications

2.02.005 Computer Use and Procedure Policy

PURPOSE

To establish Departmental policies and procedures for the acquisition, installation, de-installation, maintenance, and use of computer hardware and software.

POLICY

That all employees adhere to the provisions herein regarding computer procedures. This policy is written in accordance with MOA directives regarding computer systems and equipment.

DEFINITIONS

Assigned Component: A police department unit, section or division that is assigned a Department computer through Information Systems.

Assigned Employee: A police department employee who has been assigned a Department computer.

Authorized User: An individual sanctioned by the Anchorage Police Department, through the Information Systems Section, to utilize Department computers. An individual may be sanctioned by the very nature of their training or assignment.

Computer Maintenance and Installations: Additions, modifications or deletions of any software or hardware on a Department computer, to include opening the computer's external case.

Department Computer: Any personal computer owned or maintained by the Anchorage Police Department which includes:

Desktop: A computer and monitor that are stationery.

Laptop: A portable computer running a full commercial operating system capable of running off battery power alone.

Palm: A portable, battery-operated computer that is capable of storing or sharing files.

Downloads: Copies of files obtained through removable media such as floppy disk, CD ROM disk, etc., or files received from another computer or the Internet.

Electronic Mail (E-mail): Electronic messaging sent from one person via computer to another. Types of e-mail include:

Departmental E-Mail: Electronic messaging sent from one department to another department.

Internet E-Mail: Electronic messaging sent from one person via Internet to another.

Attachments: Electronic files sent with Department or Internet e-mail.

E-Mail Groups: Two types of e-mail groups may be authorized. They are:

Global: Groups that reside on a server and are maintained by Information Systems.

Personal: Groups that reside on individual computers in a user's address book.

IS: Abbreviation for Information Systems. That section of the Anchorage Police Department responsible for planning, purchasing and maintenance of all computer equipment, software and peripherals.

Log-in (Log-on) Access: Access to applications, files, peripherals and Department computers through the use of assigned user names and passwords for security purposes.

Log off (Log-out): The process of removing access to specific files or data. A new log-in is required to regain access.

Network: A system of interconnected computers that allows the sharing of files, software, printers, or peripheral equipment. Related items include:

Dial-up Access: The ability to access computers and files attached to a police LAN through software, security and a telephone modem, typically from a remote location.

Internet: The global system of networked computers around the world.

Local Area Network (LAN): A group of computers connected together that have the ability to share files.

Modem: A device used to send and receive electronic information (documents, images, files) from a computer, usually through a telephone line.

Wireless: The ability to connect and send/receive files by means of radio signal (e.g., cellular phone system, cellular digital packet data, or other means).

Peripheral Equipment: Any equipment attached to a computer system (e.g., scanners, printers, cameras, CD-ROM drives).

Removable Media: Any device that stores information that can be removed from one computer and moved to another (e.g., floppy disks, CD-ROM disks, thumb-drives).

Software: The instruction set used to make the hardware (central processing chips, monitors, drives, etc.) perform tasks. Some examples include:

Applications: Electronic code that performs a specific task on a computer (e.g., Microsoft Word®, Netscape®, etc.).

Commercial Software: Software purchased to run on a specific system.

Freeware. Software obtained from public sources at no cost.

Police/Data Software: Software developed specifically for, or data collected with the Police Department (e.g., a Suspect File).

Shareware: Software obtained through public sources, normally with limited features, periodic visual reminders to purchase, or a time-limit cutoff to prevent use without purchase.

Software Licensing: Software registered to one or more computers that is legally licensed and installed in compliance with the associated license.

Unauthorized Software: Any software whose use has not been approved by the manager of Information Systems, including software not required for job-related duties.

Uploads: Copies of files sent to another computer.

PROCEDURE

I. GENERAL

A. **Computer Crimes Unit.** The Department's Computer Crimes Unit will be exempt from this procedure and will follow its own internal unit policies on the use of computer resources.

B. **Purchases.** To purchase new software or hardware, the Section commander shall forward a request to the (IS) manager. A written justification included with the request shall include:

1. A needs analysis

2. A statement of how the equipment will benefit the Department

3. Training requirements.

C. **Grants.** When hardware or software is to be purchased through a grant, the items will be issued strictly according to the grant provisions. If (IS) support or maintenance will be required, plans to purchase and integrate the system must be discussed with the (IS) manager before submitting the grant application.

D. **Seized, Donated and Converted Computer Equipment.** Computer equipment that has been seized, donated, or converted to Department use must be approved by the (IS) manager prior to use. To initiate a review of equipment or software, component personnel must furnish a written request to the (IS) manager, which includes:

1. A description of the equipment

2. The intended use

3. A list of any software that must be installed

4. The name of the person(s) who will be assigned the equipment.

E. **Compatibility.** Before approval or denial of any request for hardware or software, the (IS) manager will review each request to establish:

1. Compatibility with the existing hardware and software

2. Compliance with software licensing agreements

3. Proper registration of all software.

F. **Response to Requests for Purchase or Integration.** The (IS) manager will respond in writing to the requesting component within fourteen (14) days with an approval or denial.

1. If the request is approved, it will be processed as soon as practical in accordance with current MOA policy regarding purchases.

2. If the request is denied, the (IS) manager will provide the details of the denial to the Section commander.

II. INSTALLATION AND DE-INSTALLATION

A. **Requests for Service.** To accomplish installation or de-installation of software or hardware, the requesting component shall furnish a written

description to the (IS) manager of the item(s) to be installed or removed. If the request is approved, it will be scheduled for service by the (IS) manager or a designated representative.

B. **Unauthorized Actions.** No software or hardware of any type will be installed, modified, upgraded, removed from, or connected to any Department computer or network, whether for official business or personal use, without the approval of Information Systems.

III. USE OF COMPUTERS

A. **General.** Computers are made available to employees for work-related activity only. Personal use of Department computers, applications, information or data stored on computers is strictly prohibited. Employees shall not reveal their password or access codes to other individuals except when necessary for computer maintenance or repair or with the permission of their supervisor.

B. **Desktop Computers.** Multiple users may share desktop computers as long as each user procures information (such as e-mail) through their own access code. At no time shall an employee attempt to gain access by any means to an unauthorized area of the Department or Municipal computer system, including, but not limited to, mailboxes, hard drives, servers, or networked software programs.

C. **Laptop and Palm Computers.** These computers are generally assigned to specific employees. Should it become necessary to share a laptop or palm computer, the following procedures shall apply:

1. Sharing a Department laptop or palm computer requires the permission of the assigned employee's immediate supervisor

2. Laptop or palm computers assigned to a specific employee shall remain with the component if that employee is transferred or terminates

3. Upon transfer or termination or an employee assigned a laptop or palm computer, the component commander shall return the computer to the (IS) manager for reassignment within that component.

D. **Software.** No person shall load software onto any Department computer for personal use or gain. Use of such software will be subject to disciplinary action. Employees who observe suspect software on Department computers shall report it in writing to the (IS) manager. If determined to be in violation of this policy, the manager shall cause the software to be removed from the computer.

E. **Peripherals.** Items such as printers, fax machines, copy machines and scanners, whether attached to a computer or used as a stand-alone device, shall not be used for an employee's personal business or communication.

F. **Security.** It shall be the responsibility of every employee assigned a computer or who shares a computer to ensure its security as well as the information stored on it whenever they are logged on to that computer or it is otherwise under their control. Every precaution must be taken to prevent its theft or unauthorized use. Therefore, employees shall, at a minimum:

1. Log off the Records Management System, e-mail, and NCIC when the computer is left unattended

2. Lock office doors when appropriate

3. Lock vehicle doors or secure laptop/palm computers in the trunk when the vehicle is unattended (If weather is a consideration, laptop/palm computers should be secured in the assigned employee's residence while off duty or out of service)

4. Notify the (IS) manager if Department computers or peripheral equipment are damaged or stolen, or if it appears unauthorized access was attempted or gained.

G. **Maintenance and Repairs.** Information Systems is responsible for all maintenance, support and repair of Department computers. Requests for service, unless critical, should be routed through the supervisor of the affected component. The assigned (IS) support personnel will evaluate and prioritize requests and reply to the supervisor. All requests must include the following information:

1. Nature of the problem

2. Date and time of occurrence

3. Priority (low, moderate, high).

H. **Inspections.** Department computers are subject to inspection by component supervisors or (IS) personnel at any time.

1. Should a component supervisor, through an inspection, find a violation of regulations or procedures on a computer assigned to an employee, that supervisor may be required to provide the IS manager with a written report.

2. Whenever an upgrade or maintenance is performed on a Department computer, the appropriate (IS) employee shall complete an inspection report.

I. **Training.** Certain equipment, applications or programs may require initial or recurrent training for proficiency and/or certification. Employees should request this training through the chain of command as with any other training. In any case,

1. It is the responsibility of each assigned employee to maintain National Crime Information Center (NCIC) certification if required by the employee's supervisor or job assignment; and

2. It is the responsibility of the Anchorage Police Training Academy with the assistance of (IS) personnel, to design and administer additional computer training specific to the software available to assigned employees, except for training provided by a private company approved by the Chief of Police.

IV. ELECTRONIC MAIL (E-MAIL) PROCEDURES

A. **General.** The Municipal e-mail system is a formalized communication tool that shall be used for official business only. Employees are reminded that e-mail is <u>not</u> a protected form of communication and could be subject to a discovery motion in a criminal or civil case, or constitute grounds for an internal investigation. The following procedures shall apply to all employees:

1. All employees shall check their e-mail account each business day and reply to messages that require an answer in a timely manner.

2. Employees shall disclose all passwords and codes necessary to access their personal e-mail account to a supervisor in their chain of command upon request.

3. Employees shall not attempt to gain access to another's mailbox, except that a supervisor in an employee's chain of command may conduct an inspection of an employee's account for official business purposes only.

4. All e-mail messages shall be composed in a respectful and professional manner. Employees should remain aware of the potential for widespread distribution of any e-mail message, and of the consequences for violation of Departmental regulations.

5. Any employee who receives e-mail containing a suspicious enclosure or file from an unknown source should contact (IS) personnel before opening the file.

6. Upon termination, an employee's immediate supervisor shall notify the (IS) manager so that the user's account can be removed from the system.

7. Employees are discouraged from sending e-mails with large or numerous electronic file attachments.

8. Information Systems can maintain only a limited number of global e-mail groups. Therefore, the following criteria shall be met before a global group is approved:

    a. Each group must consist of at least ten members.

    b. The group must be intended for use by at least ten employees or others.

    c. Changes to the member list should not be required on a regular basis.

    d. The group is necessary for use by an outside agency (Prosecutor, etc.).

9. Exceptions to the above have been authorized by the (IS) manager.

    a. Personal e-mail groups initiated and maintained by users are encouraged.

    b. Employees are encouraged to empty their deleted items folder on a regular basis to conserve network resources. The e-mail server will purge the DELETED e-mails after 30 days.

    c. Outgoing e-mail messages are limited in size to 40Mb to Municipal recipients and 20Mb to non-Municipal recipients. Mailboxes kept on the e-mail server are to be limited in size to 300Mb. Once that limit is reached, employees will only be able to read and receive e-mail but not be able to send e-mail.

    d. Command-level approval must be obtained before sending e-mail to the "All Personnel" and "All Sworn" e-mail groups. Command-level here is defined as a Lieutenant and above or a non-sworn UNIT supervisor.

V. INTERNET ACCESS AND USE

A. **General.** The Internet is a tool for research and communication. As such, certain employees have been granted access for business use only. Employees who abuse Internet access privileges may be subject to disciplinary action.

B. **Requests for Access.** Unless blanket access has been granted to a component, individual employees must request Internet service on an assigned computer through their immediate supervisor, who shall forwarded the

necessary documents through the chain of command. All requests must be approved by the Chief of Police.

C. **Use of the Internet.** Employees who have been granted Internet access privileges shall be subject to the following regulations:

1. Employees shall log off the Internet unless actively seeking information.

2. Employees shall not access any web site unrelated to job duties

3. Employees shall not download information or data for personal use.

4. Internet pages or web sites shall not be linked to the APD home page unless first approved by the (IS) manager.

*****END OF DOCUMENT*****