

Columbus Police Division Directive	EFFECTIVE	NUMBER
	May 15, 1993	3.63
	REVISED	TOTAL PAGES
	Dec. 30, 2007	8
Division Computer Systems		



Cross Reference:

I. Definitions

A. Executable File

A program or file that automatically performs computer functions once opened, executed, or run.

B. *Law Enforcement Databases*

Any program or source of data accessed or used by Division personnel for law enforcement purposes. This includes but is not limited to Accurant, LEADS, and OHLEG.

C. Local Operation

Computer use while not connected to the PoliceNET network. Use of internal drives A, B, C, D, or any other locally installed storage devices.

D. MailMarshal

An email security application used to filter for unauthorized content.

E. Network Operation

Logging onto, or use of, a Division workstation, application, or program linked to or installed on a network server via PoliceNET.

F. PoliceNET

The totality of the Division's network and computer equipment, software, configurations, and users.

G. PoliceNET Operations Administrator

Person(s) responsible for operation and/or maintenance of PoliceNET, including software, servers, network hardware, and connected equipment.

H. Project

Any change or addition to any Division computer, workstation or the network, including installation of software or hardware that impacts the network. This does not include repairs, relocating computers, or the purchase of computer parts.

I. *Scripting Language*

Programming languages that control a computer's applications.

J. Software

Any removable magnetic media, optical media, floppy disk, tape, CD-ROM, or program that resides on or can be copied to computer storage devices/media for use in or written in a computer-readable language.

K. Unigate

The software for connecting to the City of Columbus Unisys mainframe and LEADS.

L. Windows

An operating system that allows use of a workstation and connectivity to PoliceNET.

M. Windows Server

A network operating system for interconnecting desktop computers within the local area network.

N. Workstation

All computer-related hardware components and the area immediately around them intended for use by Division personnel. Hardware components include, but are not limited to: processor, keyboard, monitor, printer, mouse, cables, connectors, adapters, telephones, and any other device attached to any component

II. Policy Statements

A. General Operation

1. All files, including email messages and Internet logs shall be subject to public records requests. Email and other computerized records are monitored and can be retrieved at a later time for use in criminal, civil, or investigative action. Personnel do not have a reasonable expectation of privacy when using a computer or communications system that is employer-authorized or is provided for a mutual benefit.
2. Personnel shall not knowingly or recklessly delete, erase, copy, move, or format drives, **databases**, directories, disks, or files not solely used by themselves or without privilege to do so from the file(s) originator, system administrator, immediate supervisor, or author. A bureau/section/unit's network directory structure shall be reconfigured only by or at the direction of the PoliceNET Unit. Access rights to directories or sub-directories, other than those belonging to the user, shall require the approval of the bureau commander.
3. Personnel shall not copy or otherwise create an image of any program or file purchased, used, or created by the Division or Division personnel for sole use within the Division unless such copy is intended for use as a backup.

4. Personnel shall not purchase any hardware to be installed or used on a Division workstation without prior authorization from the Technical Services Bureau Commander. Personnel receiving authorization shall contact the PoliceNET Unit to make installation arrangements.
5. Only software authorized by the PoliceNET Unit shall be purchased for or installed, loaded, or otherwise used on a Division workstation or server. Personnel shall abide by all software copyright and licensing laws. Failure to do so may be a criminal and/or departmental violation.
6. Software approved for use but not supplied by the Division shall be scanned for virus contamination prior to installation or use on a Division workstation.
7. Personnel shall not remove any software owned by the Division or applications written for the Division from within the confines of Division property except to transport to another Division facility.
8. Personnel shall not configure, modify, partition, or alter any predefined hardware setting, hard disk, or software configuration located in any system. This does not apply to user defined-settings.
9. Personnel experiencing difficulty in operating a workstation shall not turn off or unplug the computer without first contacting the PoliceNET Unit Help Desk for instruction on proper shutdown procedures.
10. Unless otherwise directed by PoliceNET Unit personnel, all workstations shall be left powered 'on' and displaying the log-on screen. The computer monitor of a workstation may be turned off if the workstation is not going to be in use for more than eight hours.
11. Personnel shall save all documents/files to the PoliceNET servers. In addition, personnel may store copies locally. Repairs to or replacement of workstations may cause total loss of data stored locally and may occur with little or no notice. Network/server files are backed-up on a daily basis. The PoliceNET Unit shall not be responsible for any information/files not saved to the servers.
12. Personnel not actively using an application shall exit the program. This does not apply to locally stored applications.

B. PoliceNET Computer Network Access

1. Division personnel requesting access or changing assignments shall complete and forward a PoliceNET Computer Network Access Request, form S-20.101.
2. Access rights shall be periodically evaluated by the PoliceNET Unit supervisor and the PoliceNET Operations Administrator in order to maintain the optimum performance of the computer network.

C. Security Issues

1. Network/sign-on passwords shall be randomly created by a password generation program.

2. Personnel attempting to access the network using an invalid password shall be locked out of the network. Any user locked out shall immediately notify the PoliceNET Unit. PoliceNET Unit personnel shall investigate the cause of the lock out and determine whether access privileges should be granted.
 3. Personnel shall not communicate or divulge network/sign-on passwords to others.
 4. Personnel shall not operate or allow the operation of any network/system terminal while utilizing a password or access privilege assigned to another person.
 5. Personnel shall not leave workstations unattended without logging out, signing off, or locking the computer.
 6. Personnel not authorized to use the network or computer workstations shall not attempt to access any restricted, password-protected, or other secured file, directory, or drive.
 7. Personnel without privilege or authorization shall not use, attempt to use, or access any network computer or workstation.
 8. No computer with network access shall be equipped with or attached to any external communication device designed for remote operation or connection (i.e., a modem) without prior written authorization from a PoliceNET Unit supervisor.
 9. No computer with network access and equipped with an external communication device (i.e., a modem) shall be left in an operational mode (i.e., Host Mode) without prior written authorization from a PoliceNET Unit supervisor. This will prevent unauthorized access to the Division's network from outside sources.
 10. Personnel shall take all necessary and reasonable steps to safeguard Division computer equipment and all information/data contained therein.
 11. Personnel shall immediately report any theft, attempted theft, or loss of any Division computer equipment, data, passwords, or security cards to their immediate supervisor and to the PoliceNET Unit.
- D. Programming
1. All requests for applications or custom programming shall be made through the project initiation request process. A supervisor shall make any requests for large projects.
 2. No programs or software shall be written or purchased outside of the PoliceNET Unit without prior approval of the Technical Services Bureau Commander.
- E. Stand Alone/Covert/Wireless Networks
1. All requests for stand alone/covert/wireless networks shall be made through the project initiation request process.

2. Stand alone/covert/wireless networks shall be implemented only with the approval of the Technical Services Bureau Commander.

F. Email

1. Email shall be used for Division business purposes only.
2. Personnel shall check their email for new messages at least once during their shift. Electronic subpoenas shall be opened immediately by double-clicking the message, thereby generating a read receipt.
3. Personnel shall not attempt to access another person's email. This does not apply to PoliceNET Unit personnel acting in an official capacity.
4. Requests for information from any employee's email made by other Division personnel shall require approval of the Support Services Sub-division Deputy Chief. This does not apply to email audits by PoliceNET Unit personnel or public records requests.
5. The PoliceNET Unit shall conduct unannounced email audits for administrative purposes to insure network integrity and security. Audits will check for malicious or prohibited programs and the amount of server space used by stored email.
6. Personnel **shall not** compose, **or** transmit, any email with a file attachment that is not for Division business purposes.
7. Personnel receiving any email with a file **attachment of unknown origin or that is not for Division business** shall:
 - a. Write down the email address of the sender.
 - b. Notify the PoliceNET Help Desk as soon as possible.
 - c. If Help Desk personnel are not immediately available, delete the entire email message without opening the attached file.
8. Personnel shall delete email messages when no longer needed or useful as long as doing so does not violate **the Ohio Public Records Act** or Division policy. Personnel with questions concerning retention schedules shall contact the Public Records Unit.
9. Personnel, other than the PoliceNET Unit, shall not compose or forward computer virus alerts. Personnel receiving virus alerts shall forward a single copy of the email to the PoliceNET Unit Help Desk.
10. Personnel shall not send out Division-wide emails without the prior approval of a deputy chief.
11. Personnel shall not access any web mail or internet email sites from Division computers.
12. Personnel sending or expecting email that may contain an attachment or that may be composed in a scripting language, shall notify the PoliceNET Unit Help Desk to ensure delivery.

13. Personnel shall not circumvent normal channels of communication by composing, forwarding, or sending any mail via the email system in lieu of paper communications if the paper communications would be required under current directives.

G. Internet

1. All Internet transactions shall be recorded by the PoliceNET Unit and will be available to anyone requesting an audit of any user's Internet activity. Results of periodic audits by the PoliceNET Unit may be sent without notice to the user's supervisor or chain of command for review.
2. Personnel shall not download any software, browser plug-in, program, or non-document file without permission from the PoliceNET Unit.
3. Personnel shall not access any Internet site containing pornographic material, hacking tools or information, or other content not related to Division business without prior written permission from their immediate supervisor. A copy of the letter granting permission shall be forwarded to the PoliceNET Unit supervisor.
4. Personnel shall not access any streaming audio or video unless absolutely necessary for vital job functions. Any use of streaming audio or video that exceeds 15 minutes shall be reported to the PoliceNET Unit.

H. Care of Equipment

1. Personnel shall not expose any PoliceNET equipment to liquid, heat, direct sunlight, or magnetic influence, e.g., telephone headset, monitor, magnetic ID card holder, or electric motor. Personnel shall attempt to keep exposure to dust to a minimum.
2. Temperatures of 85 degrees Fahrenheit or greater may damage computer equipment. Personnel shall shut off all computer workstations in any area where excessive temperatures are observed or are reasonably believed to be occurring. Personnel shall not shut off any other network equipment without permission from the PoliceNET Unit.
3. Disassembling of computer components/workstations is prohibited unless performed as maintenance, repair, or upgrade by PoliceNET Unit personnel. This does not apply to personnel trained to replace disposable items such as printer paper, ribbons, or ink or toner cartridges or those acting at the direction of PoliceNET Unit personnel.
4. Personnel shall not unplug workstations from the surge protector.
5. Personnel shall not unplug, reconfigure, or move computer or network components from their original location without prior approval and assistance from authorized Technical Services Bureau personnel.
6. Personnel utilizing a workstation, terminal, or printer shall report any and all errors, problems, or difficulties related to hardware or software to the PoliceNET Unit Help Desk as soon as practical. Personnel shall not call other PoliceNET Unit members directly for Help Desk issues.

I. **Law Enforcement Databases**

1. **Designated LEADS administrators in the Technical Services Bureau shall have the final authority for the placement and use of LEADS/Unigate user interface equipped computers.**
2. Data accessed through **any law enforcement database** shall be restricted to the use of duly authorized law enforcement and/or criminal justice agencies for the performance of criminal justice duties. The data shall not be sold, transmitted, or disseminated to any non-law enforcement agency or unauthorized persons.
3. Personnel shall destroy all **law enforcement database** hard copy printouts when no longer needed.

J. **Division Websites**

1. PoliceNET Unit personnel shall be responsible for all Division websites.
2. Division personnel shall forward requests for changes or additions to Division websites through their chain of command to the Technical Services Bureau for approval. No changes or additions shall be made prior to receiving approval. PoliceNET Unit personnel may give standing approval on a case by case basis to an individual or unit responsible for regular updates.

III. **Procedures**

A. **Criminal History Audits**

1. **LEADS Coordinator/System Administrator**
 - a. **Review BCI/III Criminal History inquiries run by Division personnel on a monthly basis.**
 - b. **Upon request, conduct audits for investigatory purposes. Forward all reports to the requesting personnel.**

B. **Project Initiation Requests**

1. **Project Initiator**
 - a. Research the project, with input from PoliceNET Unit personnel if necessary.
 - b. Complete a Project Initiation Request (PIR), form J-10.118, and forward through the chain of command to the deputy chief. PIR's are accepted at any time; however, between November 15th and January 31st, PIR's will not be researched by the PoliceNET Unit.
2. **Technical Services Bureau Commander**
 - a. Review the project and consult with the forwarding bureau commander regarding project feasibility.
 - b. Forward the PIR to the appropriate PoliceNET Unit sergeant for further evaluation.

3. PoliceNET Unit Sergeant
 - a. Review the PIR.
 - b. Make changes as necessary and cause a feasibility study report to be accomplished.
 - c. Forward the study to the Technical Services Bureau Commander, with recommendations.
4. Technical Services Bureau Commander
 - a. Forward a copy of the completed package, including the feasibility study, to the originating bureau commander.
 - b. Forward the original package to the originating chain of command's deputy chief.
5. Chief of Police

Make a final decision regarding approval and project priority.