| Columbus Police Division Directive | EFFECTIVE May 15, 1993 | NUMBER 10.01 |
|---|---|---|
| | REVISED Apr. 30, 2022 | TOTAL PAGES 9 |
| **Division Computer Systems** | | |

## I. Definitions

A. 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, Accurint, Law Enforcement Automated Data System (LEADS), Ohio Law Enforcement Gateway (OHLEG), License Plate Reader (LPR)***, and CARFAX*** data.

B. Microsoft Exchange

A software application used by the Division to manage emails, calendars, contacts, and tasks for Division personnel.

C. PoliceNET

The totality of the Division's network and computer equipment, software, configurations, and users, as well as the official name of the Division's ***Microsoft*** Windows domain.

D. Department of Technology (DoT)

City personnel ultimately responsible for the Division's network and server infrastructure, desktop support, and other City-wide shared technology resources, including telephones.

E. 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.

F. Scripting Language

Programming languages that control a computer's applications.

G. Software

Anything that can be stored or copied electronically or virtually on any type of storage media in a network environment. This would include, but not be limited to, computer programs and data.

H. ***Microsoft*** Windows

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

I. Workstation

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

## II. Policy Statements

A. General Operation

1. All files, including email messages and internet logs, are subject to public records requests. Email and other computerized records may be monitored and could 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 originator, system administrator, immediate supervisor, or author. A bureau, section, or unit's network directory structure shall be reconfigured only by DoT 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 Technical Services Section (TSS) Supervisor or designee and the unit supervisor.
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 ***a*** copy is intended for use as a backup.
4. Original media for desktop software shall be provided to DoT Desktop Support personnel for safekeeping and license tracking.
5. Personnel shall not purchase any hardware to be installed or used on a Division workstation without prior authorization from the TSS Supervisor or designee and/or DoT. Personnel receiving authorization shall contact DoT to make installation arrangements. Personnel may use USB portable media devices, ***including*** flash drives and SD cards for work-related purposes, except where limited access exists, such as on MDCs.
6. Only software authorized by the PoliceNET Unit or DoT 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.
7. Software approved for use but not supplied by the Division or the City may be denied for installation by DoT.
8. 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.
9. 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.
10. Personnel experiencing difficulty in operating a workstation shall not turn off or unplug the computer without first contacting the DoT for instruction on proper shutdown procedures.

11. Unless otherwise directed by DoT 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.
12. Personnel should save all documents/files to the PoliceNET/DoT 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 by DoT, but it is not responsible for any information/files not saved to the servers.
13. Electronic data shall be stored locally or on a network/server managed by DoT or Division personnel. Exceptions include electronic data stored by a third party agreed upon by the TSS Supervisor or designee and under the authority of a contract between the City and the vendor.
14. Personnel not actively using an application shall exit the program (for example, Premier One). This does not apply to locally stored applications (for example, Microsoft Word).

B. PoliceNET Computer Network Access

1. Division personnel requesting access or changing assignments shall complete and forward a Computer Network Access Request, form S-20.101, or Change of Assignment Notification, form J-10.100, to the TSS Supervisor or designee.
2. Division personnel requesting a name change shall complete and forward a PoliceNET Name Change Notification, form J-10.101, to the TSS Supervisor or designee.
3. Access rights shall be determined by assignment, prior assignment, or specific duties and periodically evaluated by the TSS Supervisor or designee and/or DoT personnel in order to maintain the optimum performance and security of the computer network.
4. Other than PoliceNET Unit personnel and vendor support personnel, remote desktop/VPN access shall be authorized only with the approval of the Chief of Police and shall be subject to the procedures and policies established by the TSS Supervisor or designee and DoT.
5. Requests to immediately disable an employee's network and application access should come in written form from the deputy chief or higher in the employee's chain of command or from the Human Resources (HR) Manager to the TSS Supervisor or designee.
6. Accounts will be disabled at the time of retirement or when HR personnel notify the TSS Supervisor or designee of a separation from the Division.

C. Security Issues

1. An employee's initial network/sign-on password is created by DoT personnel. Passwords created by DoT personnel shall be immediately changed by the employee during the next logon and when prompted by the network application every 90 days.

2. Personnel attempting to access the network using an invalid password shall be locked out of the network. Any user locked out shall immediately contact the PoliceNET Unit or DoT.
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 privileges 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. Personnel shall take reasonable steps to safeguard Division computer equipment and all information/data contained therein.
9. Personnel shall immediately report any theft, attempted theft, or loss of any Division-owned computer equipment, data, or passwords. Personnel shall immediately report any theft, attempted theft,or loss of any personally owned device enabled to access the Division's network to their immediate supervisor and to the lostdevice@columbuspolice.org email address.
10. Division personnel shall not access or use personally identifiable information (for example, social security numbers) belonging to another employee except for a valid and authorized administrative or law enforcement purpose.

D. Programming

1. All requests for applications or custom programming shall be made to the TSS Supervisor or designee. A supervisor shall make any requests for large projects. Requests will be reviewed by TSS and/or DoT personnel for consideration.
2. No programs or software shall be written or purchased outside of the PoliceNET Unit without prior approval of the TSS Supervisor or designee.

E. Stand Alone, Covert, or Wireless Networks

1. All requests for stand alone, covert, or wireless networks shall be made to the TSS Supervisor or designee.
2. Stand alone, covert, or wireless networks shall be implemented only with the approval of the TSS Supervisor or designee and DoT.

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 Public Records Unit personnel, DoT, or PoliceNET Unit personnel acting in an official capacity.
4. Personnel shall not compose or transmit any email with a file attachment that is not for Division business purposes.
5. Personnel receiving any email with a file attachment of unknown origin or that is not for Division business shall delete the entire email message without opening the attached file.
6. 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.
7. Personnel receiving virus alerts shall contact the DoT Service Desk or use the TechDesk icon located on the computer's desktop to request DoT support immediately.
8. Personnel shall not send out Division-wide emails without the prior approval of a bureau commander/manager. Exceptions include emails sent by other City departments to all City employees ***that*** may include City-related business, health and wellness alerts, or City-sponsored events.
9. Personnel shall not use Division computers to access personal email unless access is required for work-related purposes.
10. 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 according to current directives.

G. Internet

1. All internet transactions may be recorded by the PoliceNET Unit and/or DoT and will be made available (if they still exist) to anyone requesting an audit of any user's internet activity.
2. Personnel shall not download any software, browser plug-in, program, or non-document file without permission from the PoliceNET Unit and/or DoT.
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 the bureau commander or higher. A copy of the letter granting permission shall be forwarded to the PoliceNET Unit ***Supervisor***. Letters or emails authorizing personnel to access pornographic material, etc. should be forwarded to the TSS Supervisor or designee.
4. Personnel should not access any streaming audio or video from a Division computer system unless the content is work-related or accessed in a manner that does not interfere with the performance of their duties or the performance of the network.

H. Care of Equipment

1. Personnel shall not expose any PoliceNET Unit equipment to liquid, heat, direct sunlight, or magnetic influence (for example, telephone headset, monitor, magnetic ID card holder, or electric motor). Personnel shall attempt to keep exposure to dust at 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.

Note: This does not apply to mobile computers.

3. Disassembling of computer components or workstations is prohibited unless performed as maintenance, repair, or upgrade by DoT personnel. This does not apply to personnel replacing disposable items such as printer paper, ribbons, or ink or toner cartridges. It also does not apply to those personnel performing computer forensics as part of their official duties.
4. Personnel shall not unplug workstations from the surge protector.
5. Personnel shall not unplug, reconfigure, or move computer or network components from their assigned location without assistance from DoT 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 DoT as soon as practical.

I. Law Enforcement Databases (LEADS, OHLEG, ***LPR, CARFAX,*** etc.)

1. 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.
2. Personnel shall destroy all law enforcement database hard copy printouts when no longer needed.
3. LEADS
   a. Designated LEADS administrators in the TSS shall have the final authority for the placement and use of LEADS user interface-equipped computers.
   b. Division personnel shall assist in maintaining the security of LEADS/NCIC and the information it contains and ensure that LEADS information is disseminated only to authorized personnel.
   c. Division supervisors, upon learning of an arrest of or criminal court action pending against a Division employee, shall notify the Terminal Agency Coordinator (TAC) in the Records Management Bureau (RMB) and the RMB Manager without delay.

d. Division personnel shall immediately report any loss, theft, modification, destruction, or breach of the system data or access of information by unauthorized persons to the TAC in the RMB.

e. Any misuse of law enforcement database information or equipment may constitute critical misconduct and/or result in criminal charges.

***4. LPR Data***

***a. Facial recognition shall not be accessed.***

***b. Division personnel shall confirm the accuracy of the information, "hit," or "alert" from the system prior to taking any action.***

***c. Division personnel shall accurately complete the required audit fields when using the system.***

***d. Division personnel shall ensure all searches are for law enforcement purposes only. Misuse of the database information, equipment, or log-in may constitute critical misconduct and/or a criminal offense.***

***e. Data should only be downloaded on a Division computer or Division-issued electronic device.***

***f. The Criminal Investigations Subdivision Deputy Chief or above shall determine when Division data will be shared with other requesting agencies and when the Division will request that other agencies share their data through the LPR contracted company.***

***g. The TSS Supervisor or designee shall serve as the system administrator.***

***5.*** Division personnel shall document the incident number, date, requestor name, subject name, and case/offense type of each OHLEG facial recognition inquiry on the appropriate log in the electronic reporting system.

J. Division Websites

1. Public-facing websites shall utilize the City's Ektron platform for consistency.
2. Division personnel shall forward requests for changes or additions to Division websites to the PoliceNET Unit webmaster.
3. Public information posted to the Columbus Division of Police website shall not be removed unless the posting of that information creates a substantial risk of harm to persons and the Division of Police has been informed of that risk. When a substantial risk of harm to persons is confirmed by any Division of Police supervisor or the Division of Police Legal Advisor, the information shall be removed from the website by PoliceNET Unit personnel without delay.

K. Requests for Employee Emails, Division Computer Records, or Audits for Investigative Purposes

1. Written approval by email or letter shall be required when requesting any of the following:
   a. Information from another employee's email
   b. Information from or copies of another employee's files stored on the Division's network
   c. Audits of another employee's use of Division computer systems and/or applications
   d. Audits of another employee's Division cell phone records
2. Requests for information or audits shall require the written direction by email or letter from:
   a. That employee's deputy chief or higher for chain of command investigations, or
   b. The Internal Affairs Bureau (IAB) Commander for IAB investigations.
3. This section does not apply to public records requests.

## III. Procedures

A. Repairs or Problems

Contact the DoT Service Desk or use the TechDesk icon located on the computer's desktop to request DoT support.

B. Criminal History Audits

1. TAC/System Administrator
   a. Review BCI/III Criminal History inquiries run by Division personnel on a monthly basis.
   b. Conduct or forward requested audits for investigatory purposes in accordance with the unit's SOP.
   c. Forward all reports to the requesting personnel.

C. LEADS Password Resets

Forward requests for LEADS password resets and LEADS access to the TAC in the RMB or to the Information Systems Analyst in the PoliceNET Unit.

D. Requests for Employee Emails, Division Computer Records, or Audits or to Suspend or Terminate an Employee's Network Access

1. Requestor
   a. Provide written approval by email or letter to the TSS Supervisor or designee detailing the information requested, any applicable timelines, and to whom the information is to be provided, or in the case of a request to suspend or terminate an employee's network access, the specific services or access to be modified.
   b. In an emergency situation, contact the TSS Supervisor or designee directly and provide written confirmation by email or letter as soon as practicable.

c. Cause written notification by email or letter of the request to be included in any subsequent administrative or criminal investigation.

2. TSS Supervisor or Designee

a. Comply with the request or assign the request to the appropriate PoliceNET Unit or DoT personnel.

b. Ensure the request is completed and the appropriate personnel are notified.

3. PoliceNET Unit Personnel

a. If unable to comply with the request or if additional clarification is needed, request direction from the TSS Supervisor or designee.

b. Complete the request and forward the information as directed.

E. Redacting Public Information from the Division Website

1. Records ***Management Bureau***

Upon receipt of a court order to seal all or part of a report that is currently on the public website, complete the Redacting Public Information From the Internet, form S-36.124, and forward it to the PoliceNET Unit.

2. Employee Requesting Redaction

Upon gaining knowledge that information listed on the Division's website creates a substantial risk of harm to persons, immediately bring the information to the attention of a supervisor.

3. Notified Supervisor

a. Upon being notified of harmful information on the website, immediately complete the Redacting Public Information From the Internet form and forward it to the TSS Supervisor or designee without delay.

Note: The Division of Police supervisor will advise the person who requested that the public information be removed from the website that, although the information may be removed from the Internet, the information is still a public record and available to anyone upon request.

b. Upon receipt of a denied request, notify the requestor of the denial.

4. TSS Supervisor or Designee

a. Review Redacting Public Information From the Internet forms and determine if the information should be removed from the Internet.

b. Forward approved requests to PoliceNET Unit personnel to remove the requested information.

c. Return denied requests to the submitting supervisor.

5. PoliceNET Unit Personnel

a. Immediately comply with court orders as detailed on the Redacting Public Information From the Internet form and remove requested information without delay.

b. Complete other requests for redaction as directed by the TSS Supervisor or designee.