

14.200 INFORMATION TECHNOLOGY

Reference:

Ohio Revised Code 2913.04(B) - Unauthorized Use of Computer Property
 Manual of Rules and Regulations, Section 2.05
 City Personnel Policies and Procedures, Chapter 9.1, Internet Access and
 Electronic Mail Policy
 City Information Security Manual
 Human Resources Policies and Procedures, Chapter 9
 Technology Management Unit Help Area on Department Intranet

Definitions:

Information Technology (IT) – the development, implementation, and maintenance of computer hardware and software systems to organize and communicate information electronically.

Internet – a vast computer network linking smaller computer networks worldwide, also known as the World Wide Web.

Intranet – a computer network with restricted access within a company or organization that uses software and protocols developed for the internet.

Software – the programs used to direct the operation of a computer, as well as documentation giving instructions on how to use them.

Hardware – the mechanical, magnetic, electronic, and electrical components making up a computer system including monitors, printers, etc.

Computer User Liaison (CUL) - Persons designated by a district/section/unit commander to act as the first line of assistance.

Helpdesk –

- Technology Management Unit (TMU) Helpdesk for hardware and software support.
- ETS Helpdesk for e-mail support.

Rebooting - Shutting down and restarting the computer.

Purpose:

Ensure the security and integrity of the Police Department's computer systems.

Ensure that computer systems are properly obtained, utilized, and maintained.

Policy:

No person shall attempt to gain access to or use any program, computer, or network for which they are not authorized. No person will modify, move, or delete any file or document unless authorized to do so. All software will be installed by or under the direction of TMU.

Personnel are accountable to the provisions of all user agreements when accessing software applications on Department computers.

All computers and information systems, including email, internet capabilities, and computer programs are for official business only. Police Department computers may not be used for games or internet music/videos.

Members will not use unlicensed software on Police Department computers. Violations can be a fifth degree felony under Ohio Revised Code.

Information:

The Technology Management Unit (TMU) is responsible for the purchase, installation, maintenance, and administration of information technology used by the Department.

Members have no expectation of privacy regarding the use of Police Department computers, files stored on Police Department computers, or email.

Procedure:**A. Procuring Information Technology (IT):**

1. TMU personnel will research all IT requests. TMU must be involved in all phases of IT procurement, including vendor management, demonstrations, planning, etc.
 - a. TMU will receive, inventory, install, and maintain all IT, equipment, licenses, maintenance contracts, and user agreements for the Department.
 - b. Purchase requests for all additional IT must be documented and supported on a Form 17IT.
 - 1) Submit the Form 17IT through the chain of command.
 - a) Email or FAX a copy to TMU.
 - b) The affected bureau commander will forward approved requests to TMU.
 - 2) TMU will:
 - a) Make recommendations on the Form 17IT as to the propriety of the IT requested.

- b) Complete the Form 630.
 - c) Submit Forms 17IT and 630 to the TMU Commander who will forward the request through the chain of command to the Resource Bureau Commander.
 - 3) The Resource Bureau Commander will either:
 - a) Approve the request and forward to Finance Section.
 - b) Disapprove the request and return the annotated Form 17IT to the affected bureau commander and the Form 630 to TMU.
- B. Trouble Shooting and Maintenance:
 - 1. If the user cannot solve the problem by rebooting, the user should contact the on-duty district/section/unit Computer User Liaison (CUL).
 - a. If a CUL is not available, call the TMU Helpdesk.
 - 1) After normal business hours, absent exigent circumstances, leave a description of the problem on the TMU Helpdesk voice mail.
 - 2) If exigent circumstances exist, contact the Emergency Communications Center (ECC) who will contact the TMU Commander or designee. If necessary, the recall of TMU personnel will be authorized.
 - 2. Users are responsible to store all files on the allocated server space.
 - a. Files should not be stored on local hard drives or desktop or other devices.
- C. Use of Computers:
 - 1. Do not use or install any hardware or software on Department computers.
 - 2. The standard Department desktop is the only authorized desktop format.
 - 3. Knowledge of unauthorized access to any computer, system, or network must be immediately reported to a supervisor.
 - 4. Users must "log in" in order to use any computer.
 - a. When not actively using the computer for any length of time, log off.
 - b. Do not turn off the computer.
 - c. Reboot computers at least once per day.

5. Supervisors will report personnel changes affecting computer use to TMU, including people no longer needing access to a computer, server folder, or email account.

D. Passwords:

1. Users are assigned secure passwords when their accounts are created.
 - a. Passwords should be at least eight characters in length and should include letters and numbers.
 - b. Passwords are not retained by TMU. TMU can issue a new password if necessary.
 - c. Passwords should be changed on a regular basis.
2. Electronic Mail (Email) logon:
 - a. Users should change their ETS assigned password at their first logon.
 - b. New email passwords must be unique and at least eight characters in length.
 - c. For email problems contact the TMU Help Desk. TMU personnel will either resolve the problem or refer the user to the ETS Helpdesk.
3. Personnel will not share or disclose passwords.

E. Electronic Mail (Email):

1. Abide by the City of Cincinnati Electronic Mail Policy.
2. Use for official business only.
3. Most email messages are public record.
 - a. Generally, access to email pursuant to a Public Records Request (see P.M. 18.120 and ORC 149.32) will occur with the employee's knowledge, in their presence, and with their cooperation.
 - b. Access without the employee's knowledge should be coordinated with TMU and ETS.
4. Email accounts must be accessed at least once per working day.
5. Users are required to maintain email accounts that do not exceed allowed storage limits. This includes deleted messages in the inbox, sent items folder, and deleted items folder.

6. Email accounts must be purged of all non-public record email prior to request for deletion. Request for deletion must be made by a supervisor.
- F. Internet:
1. Abide by the City of Cincinnati Internet Policy.
 2. Use for official business only.
 3. Users must be aware that downloading programs and email attachments can spread viruses.
- G. Use of Personal IT Appliances or Devices with Department-owned Equipment is forbidden by the City of Cincinnati IT Security Policy.