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
Information Technology Management Section Help Area on Department Intranet

Definitions:

Internet - The World Wide Web.

Intranet - The protected network of city owned computers.

Software - Computer programs such as Windows, Microsoft Office, Microsoft Exchange, etc.

Hardware - Computers, monitors, printers, etc. All peripheral devices are hardware.

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

Helpdesk -
- Information Technology Management Section (ITMS) Helpdesk for hardware support.
- Software trainer for software support.
- RCC 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 ITMS.

Personnel are accountable to the provisions of all user agreements when accessing software applications and programs 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 Information Technology Management Section (ITMS) is responsible for the purchase, installation, maintenance, and administration of information technology used by the Department except for a limited amount of equipment dedicated to Police Communications Section.

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. ITMS personnel will research all IT requests. ITMS must be involved in all phases of IT procurement, including vendor management, demonstrations, planning, etc.

    a. ITMS will receive, inventory, install, and maintain all IT, 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 ITMS.

            b) The affected bureau commander will forward approved requests to ITMS.

        2) ITMS 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 ITMS 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 ITMS.

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 ITMS Helpdesk.

      1) After normal business hours, absent exigent circumstances, leave a description of the problem on the ITMS Helpdesk voice mail.

      2) If exigent circumstances exist, contact Police Communications Section who will contact the ITMS Commander or designee. If necessary, the-recall of ITMS personnel will be authorized.

   b. If the system in question is a CLEAR-owned Regional Crime Information Center (RCIC) terminal, contact the ITMS Help Desk during normal business hours. After normal business hours, contact the Regional Computer Center (RCC) Help Desk.

2. Users are responsible to store all files on the allocated server space.

   a. Files should not be stored on local hard drives or floppy disks. Floppy disks are unreliable and should not be considered a dependable source of back-up.

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 daily.

5. Only data created with Police Department software may be stored on Department servers.

   a. Files, documents, spreadsheets, etc., of outside origin must be scanned for viruses before use on a Department computer.

6. Supervisors will report personnel changes affecting computer use to ITMS, including people no longer needing access to a computer.

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 ITMS. ITMS can issue a new password if necessary.

   c. Passwords should be changed on a regular basis.

   d. Supervisors can require that subordinate personnel provide them with their password.

   e. Department personnel are required to provide their passwords to ITMS personnel upon request, as may be necessary for the performance of official duties.

2. Electronic Mail (Email) logon:

   a. Users should change their RCC assigned password at their first logon.

   b. RCC requires the change of email passwords every 90 days.

   c. New email passwords must be unique and at least eight characters in length.

   d. For email problems contact the RCC Help Desk.

   e. Supervisors can require subordinate personnel provide them with their email password.

3. Personnel will not share or disclose passwords except at the direction of a supervisor.

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 ITMS and RCC.

4. 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.

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:

1. The Department does not permit the attachment of any personally owned IT appliances of any type (cameras, audio-recorders, printers, etc.) to Department-owned equipment, unless approved by the ITMS Commander.

2. Users must submit a Form 17IT and any licensing documents through the chain of command to the ITMS Commander. Describe the use, nature, and purpose of any personal IT devices requiring attachment to Department equipment.

3. The ITMS Commander will evaluate the request and recommend approval or disapproval, based on the particular IT appliance and how it may affect the function and security of Department equipment, operations, and security. ITMS will forward its recommendation to the Information Management Bureau Commander for review and approval.

4. Upon approval, the user will contact ITMS and arrange for the installation of hardware and software. Users will be notified of disapproval via the chain of command.

a. ITMS will participate in all initial installation and permanent removal of personal IT appliances connected to Department equipment.

b. After installation, ITMS will not perform any maintenance or support for personal IT devices. Any maintenance, support, or repair of such devices is the responsibility of the user/owner.

c. Persons requesting connection of personal IT devices to Department equipment could be financially responsible for repair of damage caused to Department equipment by personal IT devices.

6. If a personal IT device negatively affects the operation or security of Department equipment, immediately or subsequently, ITMS will recommend and request permission of the district/section/unit commander to remove offending device(s).

7. Use of personal IT devices connected to Department equipment is limited to official business only. Additionally, such use is subject to all policies, rules, and regulations of the Police Department and the City of Cincinnati.